

UNIVERSITY OF PHOENIX PRIVACY POLICY

Updated March 1, 2024

The University of Phoenix, Inc. (“**University**,” “**us**,” or “**we**”) recognizes the importance of privacy. In this Privacy Policy (the “**Privacy Policy**”), we disclose our practices with respect to the Personal Information that we collect about individuals, as well as the choices and rights individuals have with respect to their Personal Information that we have collected. “**Personal Information**” or “**Personal Data**” is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Certain states provide for different privacy rights and disclosures. These rights and disclosures are set forth in specific State-Related Addenda to this Privacy Policy.

1. [Scope](#)
2. [Definitions](#)
3. [Collection of Personal Information](#)
4. [Use of Personal Information](#)
5. [Disclosure of Personal Information](#)
6. [International Data Transfers](#)
7. [Cookies and Similar Technologies](#)
8. [Interest-Based Advertising](#)
9. [Individual Rights and Choices](#)
10. [Children](#)
11. [Security Measures](#)
12. [Monitoring of Communications](#)
13. [Third-Party Websites and Links](#)
14. [Privacy Policy Changes](#)
15. [Contact Us](#)
16. State-Related Addenda

[California](#)

[Colorado](#)

1. Scope

This Privacy Policy applies to Personal Information we collect from users of our Sites, Apps, Wi-Fi hotspots, and other online services, as well the Personal Information we collect about individuals, including current and prospective students, alumni, learners, visitors to our campuses, and others with whom we interact (e.g., Business-to-Business Representatives, as defined below), whether online, via phone, or offline in the course of providing our courses, programs, and services (collectively, our “**Services**”).

If you are an employee, contractor, or job applicant, then this Privacy Policy only applies to you when you are using our Services outside of those roles. If you are acting within your capacity as a current or former employee, contractor, or job applicant, then our collection and use of Personal Information is governed by our respective Employee Privacy, Contractor Privacy, or [Applicant Privacy](#) notices. If you are a former California employee, please contact us at office.complianceuopx@phoenix.edu for a copy of our Employee Privacy notice.

Certain Services may be subject to additional privacy policies or privacy disclosures relating to the Services provided on the Site(s) (collectively, "**Additional Policies**"). In the event of a conflict between any Additional Policies and this Privacy Policy, the Additional Policies will take precedence.

Student Educational Records. If you become a student, your educational information that is part of your educational record with us is subject to the U.S. Federal Family Educational Rights and Privacy Act ("**FERPA**"), state laws, and the University's policies (collectively, "**Student Educational Records Requirements**"). In the event of any conflict between Student Educational Records Requirements and this Privacy Policy, the Student Educational Records Requirements will take precedence. Students have the right to limit access to their Student Educational Records and to request a copy of such records, as set forth in the University's [FERPA policy](#). You may also contact us via one of the below methods:

Mail

University of Phoenix
Attn: Registrar's Office
4035 S. Riverpoint Parkway
Phoenix, AZ 85040

Phone

Admissions and Records Service Center: 800.866.3919.

2. Definitions

As used in this Privacy Policy, the following terms have the following meanings:

"Anonymized" means information that has been de-identified so that it no longer reasonably identifies, relates to, describes, and is no longer reasonably capable of being

associated with, or linked, directly or indirectly, to an individual. Anonymized information is no longer Personal Information.

“Apps” means software which may be utilized on our Sites and downloaded to or accessed through our Services.

“Business-to-Business Representatives” means agents or representatives of other companies or associations who may be contacted as part of or in relation to our Services.

“Education Partners” means other companies or institutions who may participate in various University initiatives (e.g., companies making University courses, programs, or other product/service offerings available to their customers, employees, potential employers, institutions conducting academic research or providing academic reporting, etc.).

“Service Providers” means entities that the University contracts with to provide services on our behalf.

“Site” means any website owned or operated by the University, which links to or displays this Privacy Policy.

“Social Network” or **“Social Networking”** means various Internet communication technologies provided on the Services as well as on third-party social networking websites such as LinkedIn, Facebook, Twitter, etc., that facilitate conversation and interaction between people online and includes, but is not limited to, blogs, discussion forums, wikis, chat sessions, news groups, etc.

“Social Network Content” (or **“SNC”**) means user-generated content you consent to share via a Social Network and includes, but is not limited to, Personal Information, digital sounds, and pictures that you upload to a Social Network. It also includes your Personal Information that may be displayed on other users’ Social Network pages.

3. Collection of Personal Information

We collect information about you directly from you, from third parties, and automatically through your use of our Services or interactions with us. We may combine the information we collect from these various sources.

Directly Collected Information. We collect Personal Information that you provide to us voluntarily (online or offline), including when you: respond to an advertisement;

participate in a survey or a drawing; request information; apply for admission to the University; go to receive a photo ID for one of the University campuses; register for classes; apply for financial aid; order educational or other products and Services; set up a Social Network or other Site profile; use our Services or one of our Apps (e.g., for career resources, learning assessments, or other interactive tools); use the chat, SMS, or email functionality on our Site to contact us; or otherwise interact with us online or offline. The exact nature of the Personal Information may vary depending on the type of response or service requested, but could include name, contact details, date of birth, education history, financial information, employment status, photos, interests, demographic information, and other information.

Automatically Collected Information. The Services may have and use cookies, pixels, third-party tags, scripts, log files, and other means to automatically collect information about the use of our Services and services, including (but not limited to): device information such as your hardware model, operating system, IP address, and unique device identifiers; collection date; publisher name; connection speed; day of week and time of day; language settings; country, state, city (relating to IP address, if available); domain (e.g., .com, .net, .mil, .org, .edu, etc.); web pages viewed; and email clicks or other actions taken. See the “Cookies and Similar Technologies” section below for more information. This information that we collect automatically may be linked with Personal Information to accomplish the purposes described in this Privacy Policy. In addition, we may use CCTV and other security monitoring to secure our premises, which may lead to the collection of Personal Information about visitors to our campuses. Further, when you call us or communicate with us through our Site by using our chat, SMS, or email functionality, we may record such calls and communications for quality and training purposes.

Information Collected from Other Sources. We may also obtain Personal Information from Education Partners, Service Providers, and publicly available sources, which may be combined with other Personal Information we have collected. For example, we may receive Personal Information about you from educational institutions which you have attended; financial institutions (e.g., related to student loans); government entities (e.g., related to education grants); employers (e.g., related to education or career initiatives); third-party platforms or accounts that you connect to or integrate with one or more of our Services; Service Providers that we work with to verify, update, or append data to the information that we have otherwise collected about you and to identify prospective students or other individuals who may be interested in our Services.

Categories of Personal Information Collected

While the Personal Information we collect varies (as explained above) depending upon the nature of the Services provided or used and our interactions with individuals, generally, we may collect the following categories of Personal Information:

- **Name, contact information, and other identifiers:** real name, alias, postal address, telephone number(s), unique personal identifier, online identifier, email address, account name, signature, or other similar identifiers
- **Commercial information:** records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
- **Financial information:** bank account number, credit card number, debit card number, or other financial information
- **Medical information, disability, and health insurance information:** to support specific programmatic or regulatory requirements or service requests
- **Demographic information:** characteristics such as race, ethnicity, gender, age, religion, national origin, citizenship status, and marital status
- **Education information:** information regarding past and present education, including institutions attended, years of attendance, courses of study, attendance records, grades, awards earned, degree(s) obtained, discipline records, financial aid awards and payment history, as well as assignments and other student-generated work or contributions to online discussions. The information collected from a student or potential student may include both directory and non-directory information as those terms are defined in FERPA and the University's [FERPA policy](#).
- **Government identification:** Social Security, driver's license, state ID card, and passport number
- **Internet or other electronic network activity information:** internet protocol (IP) address including, but not limited to, browsing history; search history; and information regarding a consumer's interaction with an Internet website, application, or advertisement
- **Audio, video, and other electronic data:** photos, call recordings, and CCTV footage
- **Employment history:** professional or employment-related information
- **Inferences drawn from any of above categories of Personal Information:** inferences used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, and abilities

4. Use of Personal Information

We may use the Personal Information we collect for the following purposes:

- **Administering applications, enrollment, registration, and financial services:** to review and process applications and registrations; to verify the information you provide us, determine your admissibility, register you for selected educational programs, and contact you relating to your University status; to provide financial services related to tuition payments and financial aid applications; to maintain student records; and for other related purposes
- **Providing support and services:** to provide our Services; to communicate with you about your access to and use of such Services; to respond to your inquiries; to provide troubleshooting, fulfill your orders and requests, process your payments, and provide technical support; for other customer service and support purposes; and to facilitate communications and collaboration with you and others in our University community, including through our Education Partners, Service Providers, and our social networking, community, and collaboration features. In the event you use the chat functionality on our Site, you may either chat with a live agent or a chatbot.
- **Personalizing content and experiences:** to tailor content we send or display on the Services in order to offer location customization, personalized help and instructions, and to otherwise personalize your experiences; to reach you with more relevant ads and to measure ad campaigns
- **Marketing and promotional purposes:** to administer promotions and contests; to promote our University and the Services we offer; to send you newsletters, offers, or other information regarding products or services we think may interest you
- **Analyzing and improving our services and operations:** to better understand how users access and use the Services we offer; for other research and analytical purposes, such as to evaluate and improve our Services and business operations and to develop additional programs, services, and features; and to improve student retention, our Services, and user experiences
- **Securing and protecting our assets and rights and preventing misconduct:** to protect our business operations, secure our network and information technology assets and services; to prevent and detect fraud, unauthorized access or activities, cheating, plagiarism, and other misconduct; and, where we believe necessary, to investigate, prevent, or take action regarding suspected violations of our student policies, Terms of Use, or this Privacy Policy, as well as fraud, illegal activities, cheating, plagiarism, misconduct, and other situations involving potential threats to the rights or safety of any person
- **Complying with legal obligations:** to comply with the law or legal proceedings. For example, we may disclose information in response to subpoenas, court orders, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements

- **Supporting our general business operations:** to support the administration of our general business, accounting, record keeping, and legal functions, including to analyze operational and business results and risks, to collect outstanding amounts owed, and to maintain business and Student Educational Records

Anonymized information. We may also de-identify information to create Anonymized data sets and reports in order to assess, improve, and develop our business, products, and Services; prepare benchmarking reports; and for other research and analytics purposes.

5. Disclosure of Personal Information

We may disclose the Personal Information we collect as follows:

- **Service Providers.** We may share your Personal Information with third-party Service Providers who use this information to perform services for us, including payment processors, content providers, chat providers, hosting providers, auditors, advisors, consultants, account collection agencies, advertising and marketing partners, and customer service and support providers.
- **Education Partners.** We may share your Personal Information with our Education Partners who we work with to make available certain educational services, programs, courses, career initiatives, and/or other offerings or who may be doing academic or other institutional research.
- **Business Transfers.** We may disclose or transfer your Personal Information as part of any actual or contemplated merger, sale, transfer of our assets, acquisition, financing, or restructuring of all or part of our business, bankruptcy, or similar event, including related to due diligence conducted prior to such event, where permitted by law.
- **Legally Required.** We may disclose your Personal Information as required under applicable law or in response to legal process (e.g., in response to a subpoena or court order).
- **FERPA Permitted.** We may disclose your Personal Information as permitted under FERPA.
- **Protect our Rights.** We may disclose your Personal Information where we believe it necessary to respond to claims asserted against us or to comply with legal process; to enforce or administer our agreements and terms; for fraud prevention, risk assessment, investigation, and protection of the rights, property, or safety of the University, our clients, customers, and others.

6. International Data Transfers

We operate and may process information in multiple jurisdictions, both in and outside the United States, such that some Education Partners and Service Providers may be located or process information outside of the jurisdiction in which you reside. In such cases, your Personal Information may be collected, used, disclosed, stored, and processed in these other jurisdictions for the purposes described in this policy. The data protection and other laws of the United States and other countries might differ from your jurisdiction. In addition, your Personal Information may be subject to the laws of those other jurisdictions, including lawful requirements to disclose Personal Information to government authorities.

7. Cookies and Similar Technologies

We use cookies, pixels, tags, local storage objects (also called Flash cookies), web beacons, and other technologies (which may be provided by third parties) on our Services to enable certain functionality on our Services; for security and fraud detection and prevention; to collect usage information about our Services and the emails that we send; and to personalize content and provide more relevant ads and information. We may combine the information we collect via these technologies with other information that we collect, including Personal Information.

Cookies. Cookies are alphanumeric identifiers that are transferred to your computer through your web browser for record-keeping purposes. Some cookies enable you to log in to our Services or save certain settings and preferences, while others allow us to identify usage and activities on our Services, personalize content on our Services, or deliver more relevant ads on third-party websites. Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The Help tab on the toolbar of most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. If you disable cookies, however, certain features may not be available or function properly. For more information or to update your preferences for certain third-party tags and cookies on our Sites, please see our [Preference Center](#).

Pixel tags and embedded script (also called clear GIFs and web beacons). Pixel tags are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, pixel tags are embedded invisibly on web pages. We may use these in connection with our Services to, among other things, identify the activities of users of our Services, improve ads, personalize and manage content, and gather usage information about our Services. We may also use these in HTML emails to help us analyze email response rates, identify when our emails are viewed, and determine whether our emails are forwarded. For more

information or to update your preferences for certain third-party tags and cookies on our Sites, please see our [Preference Center](#).

Local Storage Objects (LSOs). LSOs are data files that are stored locally in your browser by the websites you visit. LSOs can be used in a similar manner as cookies for a variety of purposes, such as keeping track of information you provided and remembering your preferences. Our Services may include video and content that rely on Adobe Flash Player, which uses LSOs (also called Flash cookies). If you have Adobe Flash Player installed on your computer, it can be set to reject or delete LSOs. This option is in the System Preferences on Mac OS X, in the Flash Player Control Panel on Windows®, or with the Flash Player management tools available on the Adobe website. Other types of LSOs include HTML5 Local Storage and similar technologies.

Do-Not-Track Signals. Do-Not-Track (DNT) is a browser-based signal that, when set, signifies your desire not to be tracked online. Find more information about [DNT signals](#). Our Services may not respond to all web browser based DNT signals. Some browsers and browser extensions support the [Global Privacy Control](#) (“GPC”) that can send a signal to the websites you visit indicating your choice to opt-out from certain types of data processing, including data sales. We have implemented tools such that when we detect such a signal, we will make reasonable efforts to respect your choices indicated by the GPC setting. In addition, you may disable certain cookies and opt out of interest-based advertising as explained in the “Individual Rights and Choices” section below.

8. Interest-Based Advertising

We may work with Service Providers (including, but not limited to, Adobe, Google, LinkedIn, and Facebook) to display advertising on our Sites or to manage our advertising on other websites. These third-party networks and platforms use cookies, pixel tags, and other technologies to collect information about your activities on our Services and other websites over time to provide you targeted advertising based upon your interests. Some ads are targeted to your interests and preferences, based on your browsing history and other information. Your browsing history may be followed in these cookies even if ads are not being displayed. We may also use device information, particularly in mobile advertising, to help deliver our advertising and measure ad campaign effectiveness. You may update your preferences for third-party tags and cookies on our Sites using our [Preference Center](#).

9. Individual Rights and Choices

In this section, we describe your rights and choices regarding our use and disclosure of your Personal Information.

Marketing Communications. You may [opt out](#) of receiving marketing communications from us. Additionally, you may follow the opt-out instructions in the footer of any marketing email we send or inform us of your decision to opt-out while on a call with us. Opt-out requests will only remove you from our marketing list, not from the list of any other third parties.

If you do not wish to receive text messages, you may opt out by responding **STOP** to cancel future text messages. To get help, text **HELP**. You may also request additional assistance by contacting TextMsgSupport@phoenix.edu or by calling 866-766-0766.

Social Networking Content. You may change various user settings related to sharing your Personal Information contained in any user profile you set up as part of Social Network activities furnished by us, subject to contractual, academic, legal, or technical restrictions and reasonable notice. Note that your withdrawal from Social Network activities might prevent us from providing you with certain products or services.

Cookies and Similar Technologies. Using our [Preference Center](#), you can opt out of or change your preferences for most third-party cookies and tags on our Sites, except those that are “necessary” to the proper functioning of our Sites or particular features available to you on our Sites. In addition, you may block or disable cookies for the device and browser you are using through your browser settings; however, if you do so, certain features on our Sites may not be available or function properly.

10. Children

We do not knowingly collect Personal Information from children under the age of 13. If we learn that we have collected or have received Personal Information from a child under 13 without appropriate parental consents, we will delete that information. If you believe we might have collected any information from a child under 13 without consent, please contact us via one of the methods in the “Contact Us” section below.

11. Security Measures

We have implemented security measures to protect against the loss, misuse, and alteration of the Personal Information under our control. However, no data transmission over the Internet can be guaranteed to be completely secure. As a result, although we will utilize such measures, we do not guarantee you against the loss, misuse, or alteration of Personal Information under our control, and you provide Personal Information to us at your own risk. You should always take care how you handle and disclose your Personal Information and should avoid sending Personal Information through insecure email, Social Networks, or other Internet channels.

12. Monitoring of Communications

We may monitor, record, and retain all incoming and outgoing communications for training of our representatives, for quality assurance purposes, as necessary for our records retention policy, and as required for legal purposes. This includes the monitoring and recording of communications and interactions between you and the chat functionality made available through our Sites. To the extent such communications are retained, they are retained in accordance with our records retention policy.

13. Third-Party Websites and Links

Some of our Services may contain links to websites or access to services provided by third parties who operate websites or provide services on their own behalf or on behalf of multiple entities. These third parties may collect your Personal Information and may apply their own policies on how your Personal Information is used. **Please make sure to read the policies of any websites or services you visit on the Internet carefully.** We are not responsible for the privacy practices or the content of any websites or services that are not operated by or exclusively for us, and the collection, use, and disclosure of Personal Information about you will be subject to the policies applicable on those websites.

14. Privacy Policy Changes

We may update this Privacy Policy or revise it from time to time. Your continued provision of Personal Information or use of our Services following any changes to this Privacy Policy constitutes your acceptance of such changes. If we make a material change to this Privacy Policy, we will attempt to notify you in advance of such change via a notice on our Site and/or, when appropriate, via email to you.

15. Contact Us

Should you have any questions about our privacy practices, please contact us at Office.ComplianceUOPX@phoenix.edu or by mail:

University of Phoenix
Ethics, Compliance, and Data Privacy
4035 S. Riverpoint Parkway
Phoenix, AZ 85040

16. State-Related Addenda

California Addendum

The California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”) requires us to make additional disclosures. If you are a California resident, please read this section for additional disclosures and information on rights you may have under California law. In the event of a conflict between this California Addendum and the remainder of this Privacy Policy, this section shall take precedence for California residents. Terms used in this section and not defined have the meaning given in the [CCPA](#).

Categories of Personal Information Collected. In the prior 12 months, we may have collected the types of Personal Information described in the “[Categories of Personal Information Collected](#)” section above. The Personal Information in this section falls into the following categories of Personal Information:

- Name, contact information, and other identifiers
- Customer records as described in California Civil Code 1798.80(e)
- Protected classifications
- Commercial information
- Biometric information
- Internet or other electronic network activity information
- Geolocation data
- Audio, video, and other electronic data
- Employment history
- Education information
- Inferences drawn from any of above
- Sensitive Personal Information

Sources of Personal Information. We collect the above categories of Personal Information from those sources set forth in the “[Collection of Personal Information](#)” section above.

Purposes for Collecting Personal Information. We collect the above categories of Personal Information for the purposes set forth in the “[Use of Personal Information](#)” section above.

Disclosed for a Business Purpose. In general, we may disclose the following categories of Personal Information to our Education Partners and Service Providers to support our educational and career initiatives and other business purposes:

- Name, contact information, and other identifiers
- Customer records
- Protected classifications
- Commercial information
- Biometric information
- Internet or other electronic network activity information
- Geolocation data
- Audio, video, and other electronic data
- Employment history
- Education information
- Inferences drawn from any of above
- Sensitive Personal Information

Categories of Third Parties to Whom Personal Information is Disclosed. In the last 12 months, the above categories of Personal Information may have been disclosed to the categories of third parties set forth in the [“Disclosure of Personal Information”](#) section above.

Sale or Sharing of Personal Information. While we do not disclose Personal Information to third parties in exchange for monetary compensation, we do disclose or make available Personal Information to Service Providers in order to receive certain services or benefits from them, such as when we allow third-party tags to collect information such as your browsing history when using our Services, in order to improve and measure our ad campaigns. California law may consider these activities to be the “*sale*” or “*sharing*” of Personal Information for cross-contextual behavioral advertising. The categories of Personal Information that we may “*sell*” or “*share*” as defined under California law include:

- Name, contact information, and other identifiers
- Customer records
- Protected classifications
- Internet or other electronic network activity information
- Geolocation data
- Education information
- Inferences drawn from any of above

We do not have any actual knowledge that we have sold or shared Personal Information of any consumer under the age of 16.

Sensitive Personal Information. We do not use Sensitive Personal Information for any purpose other than that reasonably anticipated to accomplish the purpose for which it is collected.

Retention. For each category of Personal Information collected, we only retain such Personal Information for as long as necessary to fulfill the purposes outlined in this Privacy Policy and as otherwise needed to address tax, corporate, compliance, litigation, and other legal rights and obligations.

Opt-Out Preferences. For information on whether and how we process opt-out signals, see the [“Do-Not-Track”](#) section above.

Individual Rights Under California Law

California law grants California consumers certain rights and imposes restrictions on businesses as set forth below. **If you are a resident of California, you have the following rights:**

Do Not Sell or Share. The right to opt out of the “*sale*” or “*sharing*” of your Personal Information (as those terms are defined in the CCPA).

Verifiable Requests to Delete, Requests to Know, and Requests for Correction. Subject to certain exceptions, California residents have the right to make the following requests at no charge:

- **Request to Delete.** The right to request deletion of their Personal Information we have collected and to have such Personal Information deleted, except where an exemption applies.
- **Request to Know.** The right to request and, subject to certain exemptions, receive a copy of the specific pieces of Personal Information that we have collected about them and to have this delivered, free of charge, either (a) by mail or (b) electronically in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit this information to another entity without hindrance. California residents also have the right to request that we provide them certain information about how we have handled their Personal Information, including the:
 - Categories of Personal Information collected;
 - Categories of sources of Personal Information;
 - Business and/or commercial purposes for collecting, selling, or sharing their Personal Information;

- Categories of third parties with whom we have disclosed or shared their Personal Information;
- Categories of Personal Information that we have disclosed or shared with a third party for a business purpose;
- Categories of third parties to whom their Personal Information has been sold and the specific categories of Personal Information sold to each category of third party.
- **Request to Correct.** The right to request that we correct inaccurate Personal Information.
- **Right to No Discrimination.** You also have the right to not receive discriminatory treatment if you elect to exercise the above rights.

How to Exercise Your California Consumer Rights.

Do Not Sell or Share My Personal Information Requests. To exercise your right to opt-out of the sale or sharing of your Personal Information for cross-contextual behavioral advertising, you may [submit your request](#).

Note: We will also treat Global Privacy Control browser signals as opt-out of sale/sharing requests in accordance with the do-not-track section above.

Submitting a Verifiable Request. You may [submit your verifiable request](#). Alternatively, you may call 866-809-3444 (US Toll Free).

Who May Exercise Your Rights. You may make a request to exercise the above rights on behalf of yourself or on behalf of a minor if you are the parent or legal guardian of the minor. In addition, you may authorize an agent to exercise your rights on your behalf, if you provide the agent with written signed permission.

Verification of Your Request. Once we receive your request, we will contact you to confirm receipt of your request, unless your request is a “Do Not Sell or Share My Personal Information” request submitted through our automated processes. We will require sufficient information from you in order to verify your identity and the authenticity of your request. If you do not provide us with sufficient information, we may request additional information to verify your identity, the identity of the data subject of the request, and the authenticity of the request. Certain types of requests may require additional verification, as we are subject to higher standards of authentication for such requests. We will only use Personal Information we collect during the verification process for the purpose of verifying your identity.

If an authorized agent contacts us to exercise the above rights, we will need to verify their identity as well as your identity. We will also require proof of your written authorization to the agent to act on your behalf, unless the agent holds a lawful Power of Attorney under applicable laws, in which case we will require evidence of such Power of Attorney.

We may deny your request as permitted or as required by law.

We may charge a fee to process or respond to your request if it is excessive, repetitive, or manifestly unfounded.

Colorado Addendum

The Colorado Privacy Rights Act (“CPA”) requires that we make additional disclosures to consumer residents of Colorado. In the event of a conflict between this Colorado Addendum and the remainder of this Privacy Policy, this section shall take precedence for Colorado residents. Terms used in this section and not defined in this Policy have the meaning given in the CPA.

Individual Rights Under Colorado Law

The CPA grants Colorado consumers certain rights and imposes restrictions on businesses as set forth below. **If you are a resident of Colorado, you have the following rights:**

- **Right to Opt Out of the Sale of Personal Data or Processing of Personal Data for Targeted Advertising.** We do not sell any Personal Data for monetary consideration. You have the right to opt out of the processing of your Personal Data for targeted advertising. To exercise this right, you may [submit your request](#).
- **Right to Request Access.** You have the right to request confirmation whether or not we are processing your Personal Data and to access such Personal Data.
- **Right to Data Portability.** Subject to certain exemptions, you have the right to receive a copy of the specific pieces of Personal Data that we have collected about them and to have this delivered, free of charge, once per year either (a) by mail or (b) electronically in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit this information to another entity without hindrance.
- **Request to Delete.** The right to request deletion of certain of your Personal Data that we have collected and to have such Personal Data deleted, except where an exemption applies.

- **Right to Correction.** The right to request that we correct inaccuracies in your Personal Data.

Sensitive Data. Due to the nature of our Services, we may be required to collect, process, disclose, and maintain Sensitive Data, including racial or ethnic origin, mental or physical health conditions, or citizenship or citizenship status pursuant to, and in compliance with, our obligations under federal and state laws, rules, or regulations. If we process your Sensitive Data for any other reason, we will only do so with your consent.

Profiling. We do not engage in profiling in furtherance of our decisions that produce legal or similarly significant effects, such as decisions that result in the provision of financial aid or other financial services, education enrollment or opportunity, or access to our Services.

How to Exercise Your Colorado Consumer Rights.

Submitting a Verifiable Request. You may [submit your verifiable request](#). Alternatively, you may call 866-809-3444 (US Toll Free).

Authentication of Your Request. Once we receive your request, we will contact you to confirm receipt of your request, unless your request is a “Do-Not-Sell” or “Opt-out” request submitted through our automated processes. We will require sufficient information from you in order to verify your identity and the authenticity of your request. If you do not provide us with sufficient information, we may request additional information to verify your identity, the identity of the data subject of the request, and the authenticity of the request. Certain types of requests may require additional verification, as we are subject to higher standards of authentication for such requests. We will only use Personal Data we collect during the verification process for the purpose of verifying your identity.

You have a right to submit requests to exercise your rights using an authorized agent, in which case you must still verify your identity directly with us. We may deny a request from an authorized agent if we do not have proof that they are authorized by you to act on your behalf. Furthermore, a parent or legal guardian may make a request on behalf of their child.

We may reject or deny your request as permitted or as required by law.

Appeal. If we reject or deny your request, you may appeal our decision within 30 days of receiving our denial by responding directly to the communication denying your request

or by submitting your appeal to Office.ComplianceUOPX@phoenix.edu. If you have concerns about the result of the appeal, you may contact the Colorado Attorney General.

Discrimination and Incentives. The CPA prohibits discrimination against those who exercise their rights under the law; however, the law does allow for us to charge a reasonable amount if an individual is requesting any information for an additional time within a 12-month period.