University of Phoenix Policy
Applicant Privacy

Effective: 1/6/2023	**Supersedes:** Applicant Privacy, V1 3/30/2021
Policy Owner: Ethics, Compliance, and Data Privacy	**Version Number:** 2

1.0 Overview

This policy describes our collection and use of your Personal Information in the context of reviewing, assessing, considering, managing, storing, or processing your application or otherwise considering you for a position with the University. Please note that we maintain separate policies regarding confidentiality, acceptable use, and monitoring of University-provided devices and communications systems.

2.0 Scope

All persons seeking employment with the University

If you reside in California, please refer to the Addendum of State Information for state-specific information.

3.0 Personal Information

For the purposes of this policy, "Personal Information" is any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

Please note that this policy does not address or apply to our collection of protected health information (or "PHI"), consumer credit reports and background checks, or publicly available data lawfully made available from state or federal government records. This policy also does not apply to the Personal Information we may collect from contractors, job applicants, consumers, or end users of University products and services, including employees in the context of their personal use of such products and services.

4.0 Policy

Categories of Personal Information Collected and Purposes for Use
The categories of Personal Information we collect and our use of Personal Information may vary depending upon the circumstances, such as stage of application process or the role(s) applied for. The information in this policy is intended to provide an overall description of our collection and use of such information.

Generally, we may collect the following categories of Personal Information about you:

Name, Contact Information, and Other Identifiers: real name, alias, postal address, telephone number(s), internet protocol (IP) address, email address, social security number, driver's license number, passport number, or other similar identifiers.

Purpose(s) for Use Include:
- Scheduling and conducting interviews
- Identifying candidates, including by working with external recruiters

- Reviewing, assessing, and verifying information provided to conduct criminal and background checks and to otherwise screen or evaluate applicants' qualifications, suitability, and relevant characteristics
- Extending and negotiating the terms of offers
- Administering and monitoring compliance with the University's policies and procedures
- Communicating with applicants regarding their applications and/or about other similar position(s) in which they may be interested
- Maintaining applicant personal information for future consideration
- Facilitating financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or complying with legal obligations, and for other internal business purposes
- Complying with applicable legal obligations such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Protected Classifications: characteristics of protected classifications under state or federal law such as race, color, gender identity, sexual orientation, age, religion, national origin, disability, and citizenship status.

Purpose(s) for Use:

- In support of the University's equal opportunity employment policy and diversity and inclusion efforts
- Administering University policies relating to disability accommodation, pursuant to applicable federal, state, and local laws
- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Usage Data: internet or other electronic network activity information related to your use of any University device, network, communication systems, or other information resource, including, but not limited to, browsing history, search history, information regarding your interactions with our websites, applications, or advertisements, physical and network access logs, and other network activity information.

Purpose(s) for Use:

- Auditing and assessing University operations
- Monitoring for, preventing, and investigating suspected or alleged misconduct or violations of University policies and procedures
- Administering and monitoring compliance with the University's policies and procedures
- Monitoring for, preventing, investigating, and responding to security and/or privacy incidents
- Monitoring activities, access, and use to ensure the security and function of the University's systems and assets
- Securing the University's offices, premises, and physical assets, including through the use of electronic access systems and video monitoring

- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Geolocation Data: precise geographic location information about a particular individual or device when used to access a University network, application, or other information resource.

Purpose(s) for Use:

- Securing the University's offices, premises, and physical assets through the use of electronic access systems and video monitoring
- Protecting the health and safety of the University community by minimizing the risk of exposure to communicable illnesses during a pandemic or other national or local health emergency consistent with recommendations and guidance from local, state, and federal health authorities
- Administering and monitoring compliance with the University's policies and procedures
- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Audio, Video, and Other Electronic Data: audio, electronic, visual, or similar information such as, CCTV footage from University facilities, photographs, and audio and/or video recordings (e.g., recorded meetings or webinars).

Purpose(s) for Use:

- Auditing and assessing University operations
- Monitoring for, preventing, investigating, and responding to security and/or privacy incidents
- Administering and monitoring compliance with the University's policies and procedures
- Monitoring for, preventing, and investigating suspected or alleged misconduct or violations of University policies and procedures
- In connection with the University's marketing efforts
- Securing the University's offices, premises, and physical assets through the use of electronic access systems and video monitoring
- Protecting the health and safety of the University community by minimizing the risk of exposure to communicable illnesses during a pandemic or other national or local health emergency consistent with recommendations and guidance from local, state, and federal health authorities

- Conducting audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations, and for other internal business purposes such as administration of our records retention program
- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Employment Information: professional or employment-related information.

Purpose(s) for Use:

- Scheduling and conducting interviews
- Identifying candidates, including by working with external recruiters
- Reviewing, assessing, and verifying information provided to conduct criminal and background checks and to otherwise screen or evaluate applicants' qualifications, suitability, and relevant characteristics
- Extending offers, negotiating the terms of offers, and assessing salary and compensation matters
- Administering and monitoring compliance with the University's policies and procedures
- Communicating with applicants regarding their applications and about other similar position(s) in which they may be interested
- Maintaining applicant personal information for future consideration
- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Education Information: information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

Purpose(s) for Use:

- Identifying candidates, including by working with external recruiters
- Reviewing, assessing, and verifying information provided to conduct criminal and background checks and to otherwise screen or evaluate applicants' qualifications, suitability, and relevant characteristics
- Extending offers, negotiating the terms of offers, and assessing salary and compensation matters
- Administering and monitoring compliance with the University's policies and procedures
- Communicating with applicants regarding their applications and about other similar position(s) for which they may be interested
- Maintaining applicant personal information for future consideration

- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Profiles and Inferences: inferences drawn from any of the information identified above (excluding protected classifications) to create a profile about an applicant reflecting the applicant's preferences, characteristics, attitudes, abilities, and aptitudes.

Purpose(s) for Use:

- Identifying candidates, including by working with external recruiters
- Reviewing, assessing, and verifying information provided to conduct criminal and background checks and to otherwise screen or evaluate applicants' qualifications, suitability, and relevant characteristics
- Extending offers, negotiating the terms of offers, and assessing salary and compensation matters
- Administering and monitoring compliance with the University's policies and procedures
- Communicating with applicants regarding their applications and about other similar position(s) in which they may be interested
- Maintaining applicant personal information for future consideration
- Protecting and defending the University's rights and interests and those of third parties, including managing and responding to employment-related and other legal claims or disputes and otherwise establishing, defending, or protecting the University's rights or interests or the rights and interests of others, including in the context of anticipated or actual litigation with third parties
- Complying with applicable legal obligations, such as responding to court orders, subpoenas, or other requests for information from government agencies, as well as assessments, reviews, and reporting relating to such legal obligations, including under privacy laws, employment and labor laws and regulations, and other applicable laws, regulations, opinions, and guidance

Information We Disclose to Others

To carry out the purposes listed above, we may disclose Personal Information to the appropriate personnel within the University, including, without limitation, Human Resources and Payroll/Accounting, and managers as well as University affiliates and consultants to support our Human Resources functions. We may also disclose Personal Information to third-party service providers related to recruitment, employment, and suitability screening processes as well as those that support our Human Resources functions. These third-party service providers may collect or have access to information about you only for the purpose of performing services specified in the applicable service contract, and we require these providers to undertake reasonable security measures to protect your data.

In addition, we may disclose certain Personal Information to other third parties, such as law enforcement, as required by law; to protect our legal rights to the extent authorized or permitted by law; or in an emergency where your health or safety or that of others may be endangered.

How Long We Retain Information
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 policy and as otherwise needed to address tax, corporate, compliance, litigation, and other legal rights and obligations.

Safeguarding the Information We Collect
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. You should always take care how to handle and disclose Personal Information and should avoid sending Personal Information through insecure email, social networks, or other Internet channels.

If you have any questions or concerns regarding this policy, please contact University of Phoenix Ethics, Compliance, and Data Privacy.

Addendum of State Information – California

The California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("CCPA") requires us to make additional disclosures. For applicants that are California residents, the following applies. Terms used in this section and not defined have the meaning given those terms in the CCPA.

Categories of Personal Information Collected
In the prior 12 months, we may have collected 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
- Biometric information
- Internet or other electronic network activity information
- Geolocation data
- Audio, visual, and other similar electronic data
- Professional or employment-related information
- Education information
- Inferences drawn from any of above
- Sensitive Personal Information

Sources of Personal Information
We collect the above categories of Personal Information from you, prior employers, references, and third-party recruiting providers.

Purposes for Collecting Personal Information
We collect the above categories of Personal Information for the purposes listed in the "Categories of Personal Information and Purposes for Use" section.

Disclosed for a Business Purpose
In general, we may disclose the following categories of Personal Information to our third-party service providers to support our staffing, recruiting, educational and career initiatives, and other related business purposes:

- Name, contact information, and other identifiers
- Customer records as described in California Civil Code 1798.80(e)
- Protected classifications
- Biometric information
- Internet or other electronic network activity information

- Geolocation data
- Audio, visual, and other similar electronic data
- Professional or employment-related information
- 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 listed in the "Information We Disclose to Others" section.

Sale or Sharing of Personal Information
In the last 12 months, based on our existing practices, we are not aware of having *"sold"* or *"shared"* Personal Information collected about you in the context of your employment, as defined under California law.

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 policy and as otherwise needed to address tax, corporate, compliance, litigation, and other legal rights and obligations as described in the "How Long We Retain Information" section.

Verifiable Requests to Delete, Requests to Know, and Requests for Correction
Subject to certain exceptions, if you are a California resident, you have the right to make the types of requests below at no charge.

Request to Delete: The right to request deletion of certain 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 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 (as applicable), including:
- 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; and
- 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.

Right to Correction: The right to request that we correct inaccurate Personal Information.

Submitting a Verifiable Request
You may make your verifiable request by submitting the appliable form(s) below:

- Deletion Request
- Request to Know
- Correction 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. 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.

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

Non-Discrimination
The University will not discriminate or retaliate against you if you elect to exercise the above rights.

5.0 Related Policies and Procedures

Code of Ethics

6.0 Revision History

Version	Date
1	3/30/2021
2	1/6/2023