Lindsey Wilson University
Privacy Policy

Policy 02-07

Policy
Protecting the privacy of students, vendors, and all individuals and entities doing business with Lindsey Wilson University is very important to the University and its employees. Your privacy is held in the strictest of confidence and is considered a high priority.

This Privacy Policy explains the type of information we may have about you and the type of information we sometimes share with others, as well as the type of information we will not share about you.

Information at Lindsey Wilson University is collected but not limited to the following methods

- Banner (Enterprise Resource Planning Software)
- RaiderPortal intranet (https://portal.lindsey.edu)
- Lindsey Wilson University website (http://www.lindsey.edu)
- Admissions Application (https://lindsey.elluciancrmrecruit.com/Admissions/Pages/Login.aspx)

Categories of Nonpublic Personal Information Collected by the University

- Information we receive from you on applications or other forms
- Information we receive about you from external governmental, financial, testing, or other organizations
- Information we receive in processing your accounts with us and the transactions in those accounts
- While using RaiderPortal, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to your name, address, LWU user ID and email address
- Any personal data you allow us to collect via third party sources (Google Calendar, Gmail, etc.) is only utilized insofar as is necessary to personalize your RaiderPortal experience. You may refuse to provide this information at any time, with the caveat that certain customization options and personalized features will be unavailable to you

Categories of Nonpublic Information Disclosed by the University

- Information provided to the University by you required for verification of financial aid eligibility
- Information regarding accounts that need to be available to third party contractors for collection of delinquent account balances or loans due the University or governmental loan programs
- Information requested by an authorized law enforcement process or court order
- Information to provide medical care and related insurance information for individuals covered by the University's health insurance plans

Categories of Affiliates and Nonaffiliated Third Parties to Whom the University Discloses Information
The University may disclose certain nonpublic personal information about you to nonaffiliated third parties as permitted by law. The third party must adhere to the privacy principles pertaining to such information with regard to confidentiality. The exchange of information with these entities is deemed important in order to maximize the accuracy and detail of information reported. Information is provided in the following instances:

- The customer requests the information be sent
- Disclosure is required by law

Security
The security of your Personal Information is important to us but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

The University believes that the security and accuracy of nonpublic personal information is confidential and should only be made available to persons who have a need for the information to properly provide services, act upon a request from the student or customer, or to fulfill the employee's job responsibility. If at any time you have a concern about the security or accuracy of your information, please contact the Vice President for Administration & Finance at 270-384-8040 or at Lindsey Wilson University, 210 Lindsey Wilson St., Columbia, KY 42728.

Website Acknowledgement
We use tracking technologies, including cookies, to improve the browsing experience on our website (http://www.lindsey.edu) and analyze website usage. By browsing www.lindsey.edu, you consent to our use of tracking technologies as described below.

What Data We Collect
We collect the following categories of data from www.lindsey.edu for the purposes explained below.

Data You Provide to Us
- *Hashed email addresses*: In conjunction with our third-party marketing and advertising contractor ("Contractor"), we collect hashed versions of the email addresses that visitors have entered on our site. Hashing is a technology process that pseudonymizes (i.e. digitally scrambles) email addresses. For instance, when john.doe@outlook.com is run through a typical hashing function, it becomes the following string of digits: 0F0B7B1A1A7E8BDBBC6AA545F8CCD6F83671B32479271BFCB6CC8498912058D5. We take this step to de-identify data and protect email addresses, while being able to use the unique identifier created for the purpose of recognizing you and sending you interest-based ads across different devices (computers, tablets and mobile devices) and browsers (also called "cross-device matching"). We describe cross-device matching in further detail in **How We Use the Data We Collect.**

Data We Automatically Collect from Your Device
Unless you have opted-out or have otherwise refused to provide consent, the following is data that we collect from your device automatically:
- *Device Information:* This is technical information about the device you use to access our website such as your device's IP address and operating system. Additionally, in the case of mobile devices, your device type, and mobile device's unique advertising identifier (such as the Apple IDFA or Android Advertising ID) and any other unique identifier that may be assigned to the mobile device, such as an Android ID or UDID in older Apple phone models, or a non-cookie unique identifier used by non-cookie technologies .

- *Browser Data:* This is technical information about the browser you are using that is captured in order to serve you an ad that can be rendered on your device. An example of browser information is the technical information that identifies your browser as, for example, Chrome, Firefox, Safari etc.

- *Activity on our Website:* This is data about your browsing activity on our website or application. For example, which pages you visited and when, what items were clicked on a page, how much time was spent on a page, and what site or ad brought you to our website.

- *Location Data:* This is non-precise information related to your geography derived from your device's IP address (e.g. laptop, desktop or mobile etc.). This does not reveal your precise geographic coordinates (i.e. your GPS latitude and longitude) - only country, state, city and zip/postal code level location data, and helps us to display ads that are relevant to your general location.

- *Ad Data:* This is data about the online ads we have served (or attempted to serve) to you. For example, how many times an ad has been served to you, what page the ad appeared on, and whether you clicked on or otherwise interacted with the ad.

Data We Collect from Third Party Sources

- *Campaign Performance Data:* This data includes information about how well our ads and campaigns have performed, whether on our platform or on other platforms.

- *Attribute Data:* We may collect additional information about you from other third-party sources where they have the rights to share such information and we have the rights to use it, for example, demographic data. We use this data to better understand our website visitors and to better market our offerings to you.

- *Data from Advertising Partners:* This is data that allows us to match the University cookie identifier with identifiers that may already be used by other companies in the digital advertising ecosystem that we work with ("Advertising Partners") through our Contractor, for example, ad exchanges or companies that sell advertising space on publishers' websites (sometimes referred to as "supply side platforms"). Matching cookie identifiers help us deliver ads to you and recognize you across browsers and devices, and may include pseudonymous advertising identifiers (meaning identifiers that help identify your browser or device, but not you directly) which some third party advertising platforms choose to share with us. We may work with advertising partners to synchronize their unique, pseudonymous identifiers to our own to enable us to more accurately recognize a particular unique browser or device and the advertising interests associated with it (commonly known as "ID Syncing").

How We Use the Data We Collect

We generally use the data we collect to help better identify and engage with you. For example, serve ads that aim to be more relevant to you. The data we collect also helps us measure the effectiveness of ad campaigns. Additionally, we use this data to operate and improve to serve the most relevant ads to you.

Specifically, we use this data for:

- *Interest-Based Advertising:* Selecting ads that are more likely to be relevant to you based on data such as your browsing activity, the time of day you visit specific digital properties and the time you spend on them, and non-precise geographic data inferred about your device(s).
- *Frequency capping:* Making sure that you do not see the same ad too many times. If we know you have already seen a particular ad several times, we will try to show you a different ad next time.
- *Sequencing:* If you are being served a sequence of ads, making sure we show you the right ad next in the sequence.

- *Cross-device matching:* Identifying different devices that are likely to be associated with you so that ads can be targeted, capped and sequenced across those devices, and so that campaign effectiveness can be measured and analyzed. It also helps us match devices so we can honor your opt-out choices across all devices we know are connected to the opted-out cookie. You may opt-out of cross-device interest-based targeting by employing the respective opt-out techniques we describe in **Your Choices and Opting-Out of Interest-Based Advertising and Analytics Ads**.
- *Attribution:* Monitoring when an ad is served by the University, or other third parties on behalf of the University, to enable marketing measurement. For example, being able to measure the effectiveness of a certain ad campaign.
- *Reporting:* Providing insights into how ad campaigns are performing and gaining insights into our visitors. Reporting may include ad metrics such as attribution (described above), impressions (ads served), clicks (ads you clicked on), and conversions. This data allows us to determine if an ad is not performing well, so that we will be able to see that data and update the ad.
- *Complying with Legal Process*: To satisfy in good faith any applicable law, legal process, or proper governmental request, such as to respond to a subpoena (whether civil or criminal) or similar process.
- *Investigating Wrongdoing and Protecting Ourselves or Third Parties:* To enforce our policies or investigate any potential violation of our policies, any potential violation of the law, or to protect ourselves, our students, or any third party from any potential harm (whether tangible or intangible).

Cookies and Related Technologies

The University uses cookies, tracking pixels and related technologies for the business purpose of providing services primarily for the University's marketing, advertising, or analytical services by Contractor.

Cookies are small data files that are served by our platform and stored on your device. You can refuse consent to, or opt-out of, the University cookies at any time, as explained in **Your Choices and Opting-out of Interest-Based Advertising and Analytics** below.

Specifically, the cookie we serve through the University's Contractor's Technology for this purpose is named "__adroll", "adroll_v4" and "__adroll_fpc". We may also drop cookies for the purposes described in **What Data We Collect**.

Additionally, we use **non-tracking cookies** (not unique) to store user decisions in terms of your ad consent and opt-out choices:

- We may drop an __adroll cookie with value opt-out if you opt-out as described below.
- We may drop an __consent cookie that stores the consent choices you have made regarding data processing and advertising by the University.

A full list of the University cookies is set out below:

Tracking cookies	Non-tracking cookies
__adroll	__adroll_consent_paramas
__adroll_v4	__adroll_post_consent_html
__adroll_fpc	__adroll_post_connsent_css

Non-Cookie Technology for Tracking Outside European Territories

In respect of website visitors with IP addresses not from a European Territory, the University and some of its advertising partners may use technologies other than cookie technology to recognize your computer, device or browser for the purposes of interest-based advertising, analyzing engagement with ads or content, measuring the effectiveness of a particular ad campaign or marketing effort, to monitor

against fraud or misuse of our services, or in other ways described in this policy in **How We Use the Data We Collect**. This use of non-cookie technology may be used in addition to cookies, or separately, to collect and record data about your web browsing activities on browsers, search engines or other platforms that may not utilize the University's Contractor technology.
You may opt-out of tracking via non-cookie technologies by employing the respective opt-out techniques described in **Your Choices and Opting-Out of Interest-Based Advertising and Analytics**.

Your Choices and Opting-Out of Interest-Based Advertising and Analytics
We recognize how important your online privacy is to you, so we offer the following options for controlling the interest-based ads you receive and how we use your data.
Opting out of this type of advertising will not prevent you from seeing ads, rather those ads will likely be less relevant. This is because they will not be tailored to your specific interests but will instead be based on the context of the Digital Property in which they are displayed or the ads you see may be randomly generated.
Here is how you can control how we use your data:

- *Web browser:* You can opt-out of receiving interest-based ads served by us or on our behalf by clicking on the blue icon that typically appears in the corner of the ads we serve and following the instructions provided or by clicking **here**. Please note that this "opt-out" function is browser-specific and relies on an "opt-out cookie". This means if you delete your cookies or upgrade your browser after having opted out, you will need to opt-out again.
- *Cross Device Opt-Out:* In some cases, we may link multiple browsers or devices to you. If you opt-out on a browser or device and we have additional devices or browsers linked to you, we will extend your opt-out decision to any other linked browsers and devices. Since we only link users across browsers and devices in certain conditions, there may be cases where you are still being tracked in a different browser or device we have not linked, and where we are treating you as a different user.
- Mobile Device Opt-Out: To opt-out of receiving interest-based ads that are based on your behavior across different mobile applications, please follow instructions for iOS and Android devices:
    - iOS 7 or Higher: Go to your Settings > Select Privacy > Select Advertising > Enable the "Limit Ad Tracking" setting; and
    - For Android devices with OS 2.2 or higher and Google Play Services version 4.0 or higher: Open your Google Settings app > Select Ads > Enable "Opt out of interest-based advertising"
- *Industry Opt-out Tools and Self-Regulation:*
    - Contractor is a member of the Network Advertising Initiative (NAI) and adheres to the NAI Code of Conduct. You may use the NAI opt-out tool **here**, which will allow you to opt-out of seeing interest-based ads from us and from other NAI approved member companies. In addition, the NAI opt-out tool allows you to separately opt-out of "audience matched" advertising through the NAI's "Audience Matched Advertising Opt-Out" tool. You can also use the **email opt-out tool** provided by our advertising partner to opt-out your email address from their database. Audience matching is a particular type of interest-based advertising where de-identified data (e.g. hashed emails) is tied to "offline" activity or information (this information generally is or can be associated with a consumer's email address.) To do "audience matching," we or another platform then "match" that information (in de-identified form) to cookies, mobile ad IDs, or other online identifiers. We describe this hashing activity in additional detail in **What Data We Collect**. Because this "audience matched" information is derived from an email address or information that can be tied to an email address, it is possible to opt-out with an email address. However, when you opt-out in this way, you will need to submit all the email addresses that you use for the opt-out to work.
    - We also comply with the Self-Regulatory Principles for Online Behavioral Advertising as managed by the Digital Advertising Alliance (DAA). You may opt-out of receiving personalized

ads from other companies that perform ad targeting services, including some that we may work with as advertising partners via the DAA website **here**.

- We also comply with the Canadian Self-regulatory Principles for Online Behavioral Advertising as managed by the Digital Advertising Alliance of Canada (DAAC). You may opt-out of receiving personalized ads from other companies that perform ad targeting services, including some that we may work with as advertising partners via the DAAC website **here**.

Information for California Residents Only

This section supplements the information contained in this privacy policy and applies solely to visitors, users, and others who are residents of the State of California, as defined in Section 17014 of Title 18 of the California Code of Regulations. This section is effective as of **January 1, 2020,** to comply with the **California Consumer Privacy Act of 2018** ("**CCPA**").

Any terms defined in the CCPA have the same meaning when used in this section.

Information We Collect and the Purposes for Which this Information is Used

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("**personal information**"). This collection of information is listed in **What Data We Collect**.

We set out below the CCPA categories of personal information our Contractor has collected from consumers within the last twelve (12) months in respect of marketing, advertising, or analytical services. Please note that personal information in certain categories may overlap with other categories.

	Category	**Collected**	**Details**	**Source**
A.	Identifiers	Yes	Device IP address, email address, cookie string data, pseudonymous data (e.g. hashed emails), operating system, and (in the case of mobile devices) your device type, and mobile device's identifier (such as the Apple IDFA or Android Advertising ID) and any other unique identifier that may be assigned to any device by third parties and cross-referenced to recognize a device.	Directly and indirectly from consumers, third party data providers and advertising partners.
B.	Personal information listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	Yes	*In respect of direct to consumer ("D2C") Services:* The perceived general education level of consumers may be collected for D2C marketing, advertising and analytics to the extent relevant for providing marketing or advertising.	Directly from third party data providers.

C.	Protected classification characteristics under California or federal law	Yes	Limited to age ranges such as 35-44, 45-54, 55-64 and 65+ and male/female gender categories are sometimes collected for use of Contractor's D2C Services that do not carry a risk of unintended discrimination.	From third party data providers.
D.	Commercial information	Yes	Records of products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies.	Directly from consumers and University.
E.	Biometric information	No	-	-
F.	Internet or other similar network activity	Yes	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement. For example, which pages you visited and when, what items were clicked on a page, how much time was spent on a page, whether you downloaded a white paper on a website, what items you placed into your online shopping cart, what products were purchased and the price of the products purchased.	Directly from cookie browsing history on University's website. Non-personal information about one of our ads (e.g. the third party who served the ad, and the name of the ad) may be connected with browsing history or activity on our websites for the purposes of determining attribution information (e.g. whether particular ad led to a consumer visiting our website, and, if so, which particular ad campaign).
G.	Geolocation data	Yes	Non-precise geolocation derived from IP address.	Directly from consumers and advertising partners.
H.	Sensory data	No	-	-
I.	Professional or employment-related information	No	-	-

J.	Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R Part 99))	No	-	-
K.	Inferences drawn from other personal information	Yes	Creating profiles that reflect consumer preferences and interests.	Third party data providers.

For clarity, under CCPA personal information does not include:

- Publicly available information from government records
- De-identified or aggregated consumer information
- Information excluded from the CCPA's scope such as:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data
    - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994

Purposes for Which Personal Information is Collected
All data collected is for the business purpose of providing services primarily for the University's marketing, advertising, or analytical services by Contractor. For more information on how we use this data, please refer to **How We Use the Data We Collect.**

Sharing Personal Information
We may disclose your personal information to a third party for a business purpose (as set out above) but will not sell your personal information.

Sales of Personal Information
The University does not sell personal information.

Your Rights and Choices
The CCPA provides California residents with specific rights regarding their personal information. This section describes the rights of California residents under CCPA and provides information on how to exercise those rights.

Non-Discrimination
We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services

- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties
- Provide you a different level or quality of goods or services
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services

However, we may offer you certain financial incentives permitted by CCPA that can result in different prices, rates or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information's value and contain written terms that describe the program's material aspects. Participation in a financial incentive program requires your prior opt in consent, which you may revoke at any time.

Policy History:

Origination Date: 7/2001
Revision Date: 08/1/2017, 11/18/2020