BIOMETRIC INFORMATION PRIVACY POLICY

Policy Statement

Bradley University (the "University") may collect certain biometric data from employees. This policy explains what information the University may collect, how this information may be used, how it is stored, safeguarded, retained, and disposed of.

The University utilizes a timeclock that may use biometric technology to ensure accuracy in recording time entries. Pursuant to the possible of the biometric technology, the University has instituted the following biometric information privacy policy.

Biometric Data Defined

"Biometric data" means personal information stored by the University regarding an individual's physical characteristics that can be used to identify a person, such as fingerprints, voiceprints, facial shape, or scan of hand or face geometry. Biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

Purpose for Collection of Biometric Data

The University, its vendors, and/or the licensor of the University's time and attendance software may collect, store, and uses fingerprint data to give employees access to its time and attendance system (via scanners), for employee identification, fraud prevention, and pre-employment hiring purposes.

The University, its vendors, and/or the licensor of the University's time and attendance software will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, the University's vendors and the licensor of the University's time and attendance software may be paid for products or services used by the University that utilize such biometric data.

Authorization

To the extent that the University, its vendors, and/or the licensor of the University's time and attendance software collect, capture, or otherwise obtain biometric data relating to an employee, the University must first:

1. Inform the employee in writing that the University, its vendors, and/or the licensor of the University's time and attendance software are collecting, capturing, or otherwise obtaining the employee's biometric data, and that the University is providing such biometric data to its vendors and the licensor of the University's time and attendance software;

2. Inform the employee in writing of the specific purpose and length of time for which the employee's biometric data is being collected, stored, and used; and

3. Receive a written release signed by the employee (or his or her legally authorized representative) authorizing the University, its vendors, and/or the licensor of the University's time and attendance software to collect, store, and use the employee's biometric data for the specific purposes disclosed by the University, and for the University to provide such biometric data to its vendors and the licensor of the University's time and attendance software.

Disclosure

The University stores all biometric data in accordance with applicable standards and laws.
The University will not sell, lease, trade, or otherwise profit from an employee’s biometric data.

The University will not disclose or disseminate any biometric data to anyone other than its vendors and the licensor of the University's time and attendance software providing products and services using biometric data without/unless:

1. First obtaining written employee consent to such disclosure or dissemination (See Attached Acknowledgment Form);

2. The disclosed data completes a financial transaction requested or authorized by the employee;

3. Disclosure is required by state or federal law or municipal ordinance; or

4. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The University shall retain employee biometric data only until, and shall request that its vendors and the licensor of the University's time and attendance software permanently destroy such data when, the first of the following occurs:

1. The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with the University, or the employee moves to a role within the University for which the biometric data is not used; or

2. Within 3 years of the employee's last interaction with the University.

Biometric data will be deleted from the University's timekeeping systems promptly after an employee's separation from employment with the University.

In no situation will biometric data be retained for more than three years after an employee's last interaction with the University, unless otherwise required by law.

Data Storage

Biometric data will be stored, transmitted, and protected using a reasonable standard of care for the University's industry, in a manner that is the same as or that exceeds the standards of care used to protect other confidential information held by the University. This includes, among other things, restricting access to biometric data to authorized University employees or vendors who have a business need to access the information, and using reasonable technological means to prevent unauthorized access to the information. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the University stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.

Policy Distribution and Updates

A copy of this policy will be made publicly available at https://www.bradley.edu/legal/privacy/.

Bradley University will update this policy if it begins collecting biometric data for any other purposes. Bradley University reserves the right to amend this policy at any time.

BRADLEY UNIVERSITY BIOMETRIC INFORMATION PRIVACY POLICY ACKNOWLEDGEMENT AND CONSENT

The employee named below has been advised and understands that the University, its vendors, and/or the licensor of the University's time and attendance software may collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing the University's biometric timeclocks or timeclock attachments. Biometric timeclocks are computer-based systems that may scan an employee's finger for purposes of identification. The computer system may extract unique data points and creates a unique mathematical representation used to verify the employee's identity, for example, when the employee arrives at or departs from the workplace.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), regulates the collection, storage, use, and retention of "biometric identifiers" and "biometric information." "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

The employee understands that he or she is free to decline to provide biometric identifiers and biometric information to the University, its vendors, and/or the licensor of the University's time and attendance software without any adverse employment action. The employee may revoke this consent at any time by notifying the University in writing.

The undersigned employee acknowledges that he/she has received the attached *Biometric Information Privacy Policy*, and that he/she voluntarily consents to the University's, its vendors', and/or the licensor of the University's time and attendance software's collection, storage, and use of biometric data through a biometric timeclock, including to the extent that it utilizes the employee's biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to the University providing such biometric data to its vendors, and/or the licensor of the University's time and attendance software.

_____

Employee Signature Date

_____

Employee Name (print)