BIOMETRIC INFORMATION PRIVACY POLICY

Policy Statement

Bradley University (the "University") may collect certain biometric data from students. 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 online remote testing services and examination proctoring technology which may utilize biometric technology to ensure integrity and compliance during remote testing. Pursuant to the possible use 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 remote testing software may collect, store, and use facial shape or a scan of face geometry data to monitor remote student testing, for student identification, and fraud prevention.

The University, its vendors, and/or the licensor of the University's remote testing software will not sell, lease, trade, or otherwise profit from students' biometric data; provided, however, the University's vendors and the licensor of the University's remote testing 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 remote testing software collect, capture, or otherwise obtain biometric data relating to a student, the University must first:

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

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

3. Receive a written release signed by the student (or his or her legally authorized representative) authorizing the University, its vendors, and/or the licensor of the University's remote testing software to collect, store, and use the student'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 remote testing 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 a student'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 remote testing software providing products and services using biometric data without/unless:

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

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

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 student biometric data only until, and shall request that its vendors and the licensor of the University's remote testing 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 student's enrollment with the University; or

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

Biometric data will be deleted from the University's remote testing systems promptly after a student's enrollment with the University ceases.

In no situation will biometric data be retained for more than three years after a student'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 student named below has been advised and understands that the University, its vendors, and/or the licensor of the University's remote testing software may collect, retain, and use biometric data for the purpose of remote testing and examination proctoring to ensure integrity and compliance during remote testing. Remote testing software is a computer-based system that may scan a student's facial geometry for purposes of identification. The computer system may extract unique data points and create a unique mathematical representation used to verify the student's identity, for example, when the student takes an exam administered by computer remotely.

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 student 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 remote testing software without any adverse action. The student may revoke this consent at any time by notifying the University in writing. Should the student not consent, the student is required to take any future tests in person by making arrangements with the instructor or will make alternative arrangements with the instructor. The student understands that by declining to provide biometric identifiers and biometric information, the student is required to contact the instructor to arrange for in-person testing or other such arrangements as determined by the instructor.

The undersigned student acknowledges that he/she has received the attached *Biometric Information Privacy Policy,* and that he/she voluntarily consents to the University, its vendors', and/or the licensor of the University's remote testing software's collection, storage, and use of biometric data through remote testing software, including to the extent that it utilizes the student'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 remote testing software.

_____

Student Signature Date

_____

Student Name (print)