# BIOMETRIC DATA POLICY & CONSENT

## BIOMETRIC DATA & CONSENT POLICY

### WHAT IS BIOMETRIC DATA?

Biometric data means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometrics are a way to measure a person's physical characteristics to verify their identity.

### WHY DO WE NEED TO VERIFY YOUR ATTENDANCE?

The United States Department of Education & our accreditor, NACCAS, want each school to ensure that each student's attendance has been verified. Your fingerprint is unique which makes this an ideal way for us to verify your attendance.

### FROM FINGERPRINT TO TEMPLATE

- Biometric data is first created from scanning your fingerprint.
- The system then creates a digitized template. The fingerprint is not stored.
- This template is created on each & every scan.
- Then, it is compared against the database of the digitized templates (in the system) to record your clock in & your clock out activity.

### STORAGE OF BIOMETRIC DATA

The data template is stored in a secure & encrypted database table in the KEI SIS as encrypted data and cannot be used to recreate the complete original image.

- All data used in the KEI SIS system follows the following data security protocols.
- All databases and user access are password protected & managed for security
- All information on computer screens are hidden from persons who are not authorized to see them
- All data is securely backed-up according to procedure
- All staff are annually advised of the school's security measures & compliance is compulsory
- All premises are secured when unoccupied

### USE OF BIOMETRIC INFORMATION

A fingerprint reader is a security device that uses a scanned image of your fingerprint to authenticate users in the KEI SIS system.

Fingerprint security software users can log into the application to record clock in & clock out times by scanning your fingerprint instead of typing the Username and password on the keyboard.

The biometric timeclock system enables the fast, automatic identification of students, staff & employees for authentication/verification for verifying attendance.

## RETENTION OF BIOMETRIC DATA

Fingerprint data will remain active until the student graduates or withdraws from the school. Once the student status is converted to Graduated or Withdrawn/completed in the KEI SIS system, the student fingerprint data is purged from the system.

As soon as a student permanently leaves the school his/her biometric data is immediately deleted.

## ACCESS BY OTHERS

- KEI does not sell, lease, trade, or otherwise profit from a person's or customer's biometric identifier or biometric information.
- KEI does not disclose, re-disclose, or otherwise disseminate a person's or customer's biometric identifier or biometric information unless required by law.
- KEI does not share personal information; including, but not limited to fingerprint information, with any non-vendor third party organization.

## ACCESS TO YOUR PERSONAL DATA

After initially collecting fingerprint information, there is not a user interface to view or access personal biometric data. Students are able to request access to personal data, but fingerprints, once used to create the digitized template, are not accessible or viewable.

## CONSENT

If you do not consent to using your fingerprint to verify your attendance, you will be required to use a user name & password. You may be required to provide additional assurances to support your attendance.

## FOR MORE INFORMATION

IL residents, for more information about the IL Biometric Information Privacy Act (740 ILCS 14/). Please click this link.