OUR POLICIES

Biometrics Information Privacy Policy

TABLE OF CONTENTS

Biometric Information Privacy Policy

This Biometric Information Privacy Policy applies to biometric information we collect, use and manage as part of the pixevety platform.

At Pixevety Pty Ltd ('Pixevety'), we care deeply about your privacy and the protection of personal information. We understand that biometric information is a sensitive type of personal information that requires greater protection and care.

This policy explains how we collect, use, store and otherwise manage biometric information in accordance with relevant privacy laws, including those that relate directly to the handling of biometric information.

Biometric information

Biometric information is a type of personal information. It is information that is derived using different techniques or technologies that identifies a person based on their biometric characteristics (such as facial image, retina scan, fingerprint, voiceprint).

Pixevety collects, stores, and uses biometric information derived from facial recognition technology. Where the facial recognition functionality is enabled, the pixevety platform uses one or more facial images of the person (such as a student ID photo) to identify the person where they are captured in other images within a specific gallery.

The facial recognition technology works as follows:

1. Ingests a known facial image of a person (e.g., a student ID photo)
2. Segments the facial image
3. Submits image segments
4. Conducts algorithmic measurements of key facial features
5. Translates these into an encrypted feature vector (not an identifiable image)
6. Store encrypted numerical face template for future comparison
7. Matches incoming feature vectors only within that specific gallery, and
8. Delivers result.

Our Use of Biometric Information

We collect, store, and use biometric information derived from facial recognition to identify and tag people where they are captured in images in a gallery, for the following purposes:

(a) To apply consent restrictions to images as part of our consent management module; and
(b) To allow gallery owners and members to search and retrieve a person's images (where the person has provided consent for members to access their images).

Using facial recognition technology, the pixevety platform automatically identifies a person by matching a known feature vector of the person with other images that capture the same person within a gallery. In real time, the pixevety platform 'tags' that person in an image and automatically applies consent restrictions to the image based on who has been tagged in the photo. For example, all photos tagged with Johnny Smith will be marked as 'Not for Marketing Use'.

The pixevety platform also allows gallery owners (e.g., a school) and members (e.g., school families) to search and retrieve images where a person has been tagged. A gallery owner or member can only search for images within a specific gallery, where the gallery owner has provided access to those images (i.e., through access settings). A gallery member may or may not be able to search for a person based on their consent.

We will not use or disclose your biometric information for any other purpose unless we are legally required to do so (e.g., where a court order compels us to). We will never sell, trade, or lease your biometric information for any purpose.

Our Privacy-by-Design Approach

Pixevety takes a Privacy by Design (PbD) approach when managing the privacy aspects of the platform. PbD is about ensuring that privacy and the protection of personal information is built into the design of a system or platform up front, as part of the foundational specifications, as opposed to being bolted-on at some later point in time.

The consent management module is a key Privacy by Design (PbD) feature of the pixevety platform. It is an active opt-in consent process for images, where a person can change or revoke their consent for the access and use of their images (e.g., whether a student's image can be published by a school to social media or can be searched for by other members).

Facial recognition technology allows for a customer (e.g., a school) to identify the images of a person (e.g., a student) in seconds and ensure that the person's image consent requirements can be acted upon quickly and reliably by the customer.

Consent

Depending on how you use the pixevety platform, Pixevety (or your school or sporting club) is required to:

(a) inform you about the collection of biometric information, and
(b) get your consent or permission before collecting your biometric information.

When the pixevety platform is used by an organisation (such as a school or sporting club) to manage images, Pixevety is considered a service provider to that organisation. In this scenario, the organisation is responsible for informing you of the collection and obtaining your consent before collecting your biometric information.

Where you use the pixevety platform as an individual user, Pixevety will inform you of the collection and ask for your consent prior to collecting your biometric information.

You are able to turn off the facial recognition functionality in your gallery settings at any time.

Storage and Retention of Biometric Information

Pixevety takes care to store, transmit and protect biometric information from unauthorised access and disclosure, and from loss. We apply a high level of security controls to ensure biometric information is protected in the same manner as other personal information of a sensitive nature.

CONTRACTED SERVICE PROVIDER

We use a contracted service provider to provide our facial recognition functionality, who stores data, including biometric information, in the jurisdiction in which it was collected. The biometric information is encrypted and specific to each gallery. Our provider is not permitted to handle biometric information in any way other than as expressly required to provide the service.

RETENTION

Pixevety only keeps biometric information for as long as necessary to fulfil the purpose of identifying and tagging persons in images in order to (a) apply the person's consent restrictions to those images

(i.e., as part of the consent management module) and (b) allow the gallery owner and members to search and retrieve tagged images.

You may turn off the facial recognition functionality at any time in your gallery settings. Where you turn off this functionality, we will stop using facial recognition technology to identify you in images contained within your gallery. We will also securely destroy any biometric information that we hold about you (including your feature vector).

When the pixevety platform is used by an organisation (such as a school or sporting club) to manage images, Pixevety is considered a service provider to that organisation. In this scenario, the organisation is responsible for determining how long biometric information is kept by pixevety on their behalf. Pixevety securely removes biometric information when directed to by customer organisations.

Contact Us

You can find out more about our approach to privacy and how we use facial recognition in Our Policies and our FAQs or contact us at:

Mail:

Privacy Officer
Pixevety Pty Ltd
PO Box 7056
Brookvale, NSW, 2100
Australia

Privacy Officer
Pixevety Inc.
PO Box 408333
Fort Lauderdale FL 33348
United States

Email: privacy@pixevety.com

This policy was last revised: November 26, 2021.