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.

This policy has been updated to take into account the removal of the automated face recognition feature in pixevety personal accounts.

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).

Face biometric data is the specific data that will be processed in a media gallery within pixevety.

pixevety collects, stores, and uses face biometric data derived from automated face recognition technology (AFRT). Where the AFRT 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 media gallery.

The AFRT works in pixevety as follows:

1. Ingests a known facial image of a member (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. Stores encrypted numerical face template for future comparison
7. Matches incoming feature vectors only within that specific media gallery, and
8. Delivers result.

Our Use of Biometric Information

On instruction from an Enterprise Gallery Owner (School/Education Establishment/Organisation), we may collect, store, and use face biometric data derived from AFRT for a specific purpose only, which is to store in a single controlled accessible and secure environment, school media (i.e., namely photos and videos) related to members (students, staff, child) for the sole purpose of:

(a) applying the member's photo consent in the media gallery; and
(b) allowing the Gallery Owner to search for images containing a member.

Using AFRT, the pixevety platform automatically identifies a member by matching a known face feature vector of the person with other images that capture the same person within the media gallery. In real time, the pixevety platform 'tags' that member in an image and automatically applies their media consent restrictions to the image. For example, all photos tagged with Johnny Smith will be marked as 'No Social Media'.

The pixevety platform may also enable a Gallery Owner (e.g., a school) and their invited community (e.g., school parents) to search and retrieve images in the media gallery where a member has been tagged, where the Gallery Owner has provided access to those images (i.e., through access settings). You may or may not be able to search for a member based on their media 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 media 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).

AFRT allows for a Gallery Owner (e.g., a school) to identify the images of a member (e.g., a student) in seconds to ensure that the member's media consent requirements can be acted upon quickly and reliably by the customer.

Consent

Depending on how an Enterprise Gallery Owner/Customer uses the pixevety platform, they will be required to inform you about the collection of biometric information, and get your consent or permission before collecting your biometric information (if that is the organisation's lawful basis for processing).

You can withdraw your consent at any time by communicating with the Gallery Owner.

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 (if required) before collecting your biometric information.

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, AWS Rekognition, to provide our automated facial recognition functionality, who stores data, including biometric information, in a location instructed by the Gallery Owner. The biometric information is encrypted and specific to each media gallery. No member matching occurs outside of the media gallery ensuring member data is never shared with this third-

party provider. Our provider is not permitted to handle biometric information in any way other than as expressly required to provide the service.

RETENTION

On instruction from the Enterprise Gallery Owner/Customer, pixevety only keeps biometric information for as long as necessary to fulfil the sole purpose of identifying and tagging members in images on behalf of an Enterprise in order to: (a) apply the member's media consent restrictions to those images (i.e., as part of the consent management module) and (b) allow the Gallery Owner and its invited users to search for tagged images.

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 an Enterprise Gallery Owner/Customer.

An Enterprise Gallery may turn off AFRT at any time in their media gallery settings. A member can also request to opt-out of AFRT processing at any time by contacting the Gallery Owner. Where you turn off this functionality, we will stop using AFRT to collect your face biometric data to automatically identify you in images contained within the media gallery. We will also securely destroy any biometric information that we hold about you (including your face feature vector).

Contact Us

You can find out more about our approach to privacy and how we use AFRT 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 6, 2024.