







-  **Maya Ford**  
Student
-  **Hannah Howard**  
Student
-  **Isabella Thomas**  
Student
-  **Helen Perry**  
Staff

# Photos and Face Tagging

learn  
**vidigami**

Questions? Contact us at [privacy@vidigami.com](mailto:privacy@vidigami.com)  
or visit us at [vidigami.com](https://vidigami.com)

# Photos, Face Tagging & Vidigami

Thousands of photos and videos are captured every day from teachers, administrators, students, and families showcasing learning inside and outside the classroom. Tagging whether applied manually by users or automated by artificial intelligence (AI) helps organize content with valuable contextual information to facilitate enhanced search and content discovery.

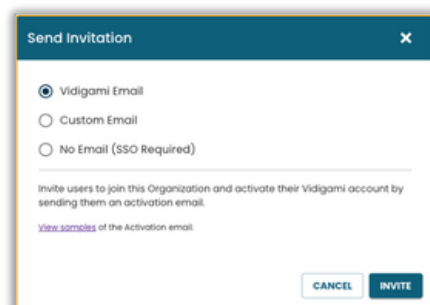
For the purposes of this document, we will be focusing on tagging used to associate an individual's name to an image.

What is ...	
People tag	A people tag is created when an individual's name is assigned to the media in which they appear. The name is associated with the media item but is not attached to a specific face. People tags are NOT assigned to detected faces. People tags are NOT face tags.
Face tag	<p>A face tag is created when an individual's name is assigned to a detected face. There are two ways a face tag can be created:</p> <ol style="list-style-type: none"><li>1.when a name is manually selected from the registered User list, or</li><li>2.when AI-enabled facial recognition technology matches a face to an individual.</li></ol>
Creator tag	A creator tag is made when an individual's name is assigned to the media they create. Like a people tag, creator tags are manually applied. The name is associated with the media item but is not attached to a specific face. Creator tags are used to attribute ownership to content production and may or may not include images of individuals.

# 5 Things to Know about Tagging in Vidigami

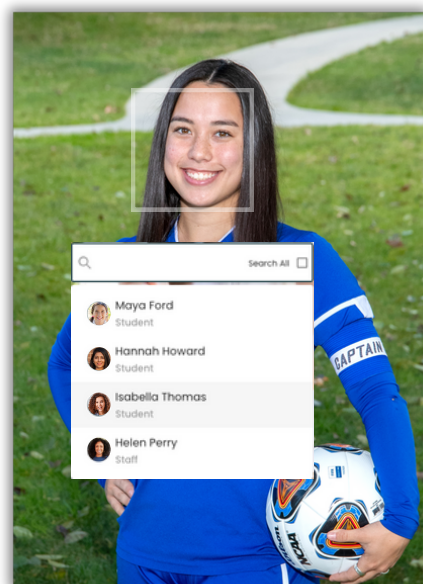
## 1. Only registered users may be tagged – manually or automatically

Users in Vidigami are authenticated by their school. Those who choose not to participate may advise their school administrator and ask to be removed from Vidigami as a registered user. This will prevent their name from appearing on the Users list for tagging. While content shared in Vidigami may include this User, they will remain anonymous because there is no option for associating the user's name with the media.



## 2. Tagging Options

Each school determines the tagging option they adopt for the school and available to their users.

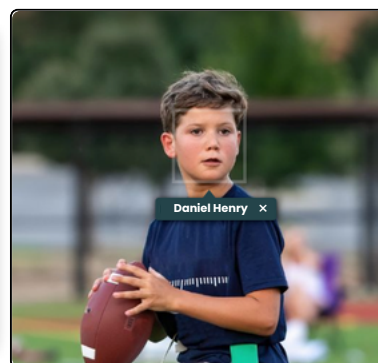
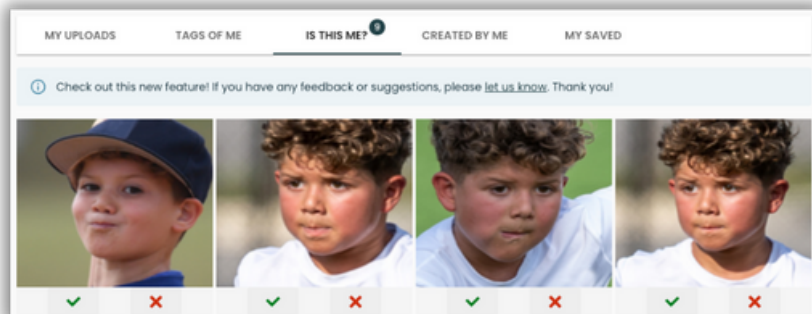


- **Automated Tagging:**  
System leverages AI- enabled facial recognition to automatically generate face matches and tagging.
- **Assisted Tagging:**  
System detects faces and prompts users to manually tag by selecting name from the User list. When a face is not detected, user may add a face box. No machine learning is used to train or process images.
- **Manual Tagging:**  
System neither detects nor recognizes faces. Users may add “people tags” to an image.

### 3. Manual vs Automated Facial Recognition

Facial recognition involves applying a name to a detected face. Applying a name to a detected face can be manual (assisted tagging) or automatic (automated tagging).

Manual recognition involves the verification of a detected face by an end user. The user will be able to select a name from the list added by the school. A user will not be able to be manually tagged if they are not in the user list in Vidigami.



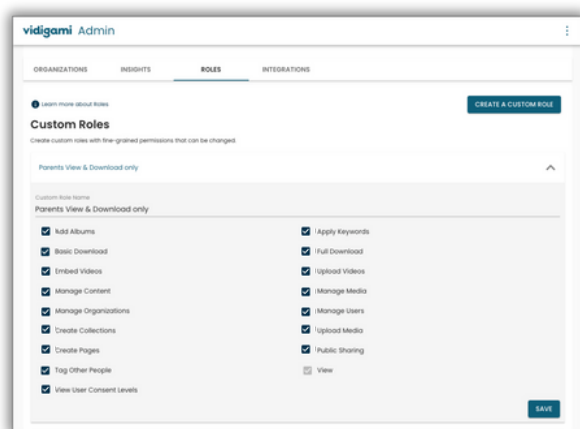
Automated recognition involves the verification of a name to a detected face through AI-enabled facial recognition. The system is instructed to train, store and generate possible matches for each detected face.

When a face is tagged, whether manually or automatically, biometric data is generated and stored. Biometric data is generally defined as image data that creates an individual profile allowing for automated image matching and identification. Any biometric data stored in Vidigami is obfuscated from the image and secured within the Vidigami system making it difficult to reassemble and associate with an image. No biometric data is downloaded with an image.

### 4. Organization permissions

In addition to the option of selecting manual, assisted or automated tagging, each school may tailor the tagging permissions available to their faculty, staff, students, and families.

By default, all users are given the permission to tag themselves and their children. A school can choose to extend this permission to permit all users to tag each other.





## 5. User Consent Management

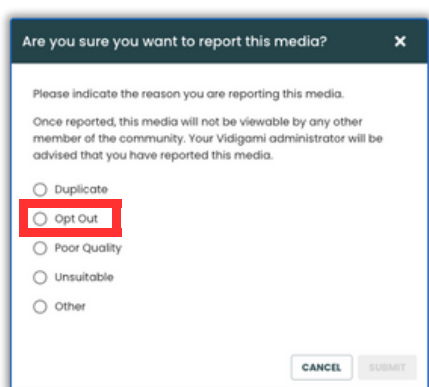
Helping schools and their community respect content ownership and personal data privacy rights are fundamental to the Vidigami system. To accomplish this, we enable each user with the ability to give and withhold consent to every photo shared in Vidigami.

**User Withdrawal** – A user or parent can decline participation in Vidigami. If a user is not registered in Vidigami, their name is removed from the user list. No face tagging, facial recognition, or people tags can be applied to media shared in Vidigami since only registered users appear on the list for tagging.



**Opt-Out** – Any user (or parent) can choose to have their child opted out of Vidigami. Opting out requires assisted or automated tagging be enabled. Once a user's face is tagged, their photos (regardless of who uploaded the image) are automatically unshared in Vidigami.

**Consent Levels** – A parent or user can restrict how their photos may be shared. If designated with "No public release" consent, that individual's thumbnail image will be highlighted in red, marking the presence of an individual who has withheld their permission for sharing their image publicly. Additional consent levels may be assigned according to each school's policies.



**Photo Removal** – All users have the right to request a photo be unshared in Vidigami for any reason. Immediately after a user makes this request, the photo is unshared with all users. Vidigami Admins can see each photo reported, the user who reported it, and the reason why.

**Manual Tagging** – A user or parent may elect to disable facial recognition so that the system does not automatically match or tag images of their child or themselves. This option is available to schools who have opted-in to use facial recognition.

# Facial Recognition & Tagging Working Together

Facial recognition is implemented to simplify the tagging process so that the process of visually documenting each student's school experience can be systematically captured. It is important to keep in mind that many photos uploaded do not provide adequate information for facial recognition to automatically tag.

For example, the 16 images below represent a typical collection of photos from the classroom, special events, field trips and sports.



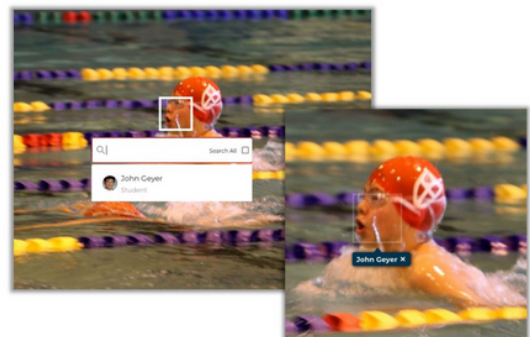
\* This assumes families have low tolerance for mistags of their children.

Finally, the faces in the last four photos cannot be detected so recognition cannot happen. When this occurs, manually tagging is required.

Make tagging part of your community engagement strategy. Empower your students, families and faculty to capture and share in the school experience that can be uniquely their own.

Notice that one-third of the photos have the potential of being auto-tagged because the face is clearly featured.

The second third feature blurry photos and profile images which reduces recognition confidence preventing auto-tagging. When face recognition falls below a confidence threshold, they require user verification.\* These photos would be presented under the "IS THIS ME" tab and users will be prompted to verify.



# Weighing the Value of Facial Recognition Technology



Each school must evaluate the risks and benefits of using facial recognition technology and decide what will work best for the school.

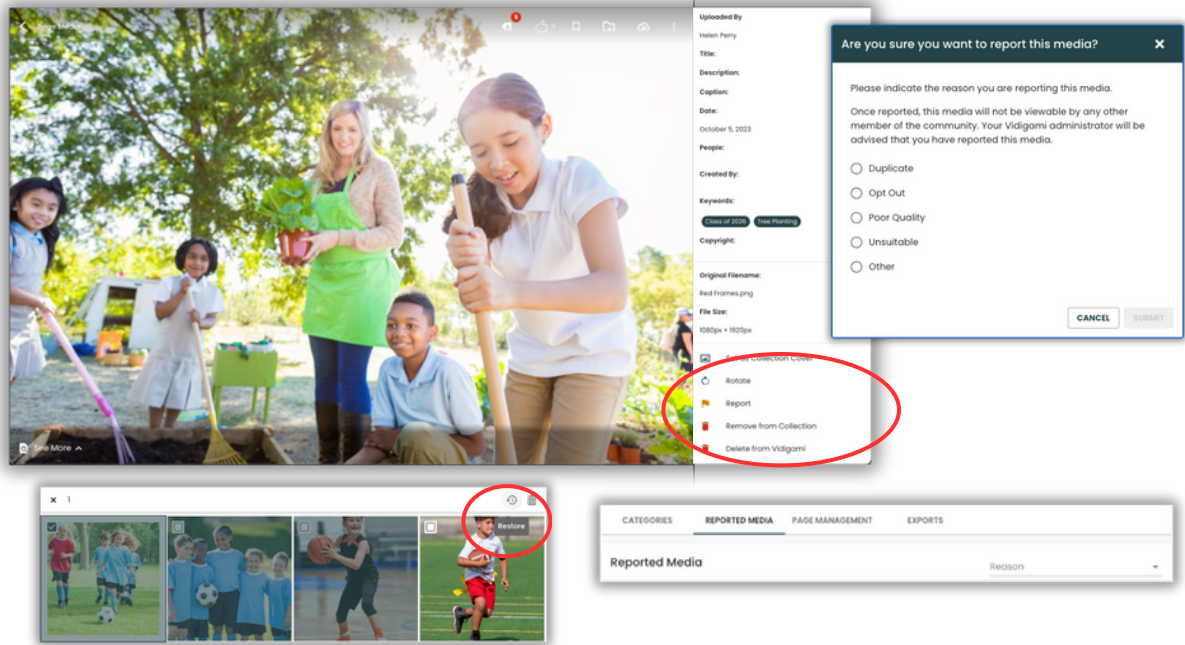
AI-enabled facial recognition leverages machine learning and biometric data to automate the process of identifying an individual and associating that individual to a name in visual media.

Using facial recognition in a closed-system such as Vidigami can be highly valuable to everyone in the school community.

Here is an excerpt from a blog published by [9ine Consulting](#), a leading cybersecurity consultancy to international independent schools that can help guide your discussion: [“How are schools coming to the conclusion that facial recognition is appropriate?”](#) In this article, [Mark Orchison](#), CEO of 9ine proposes

There are no real right or wrong answers when it comes to privacy law. There is however the expectation that a process is followed to determine the risks that are created through the processing of personal data. To follow a process, people need to be trained and the organisation needs expertise, capability, and capacity to know what it should and shouldn't be doing. Whether it be schools suffering cyber attacks, mis-handling information rights requests, or undertaking processing that shouldn't be happening, the common trend is a lack of training or expertise. Privacy technology such as that delivered and created by 9ine, and training programmes, such as those created by Educare, go a long way to building awareness, demonstrating accountability, and cost-effectively managing privacy compliance. The silver bullet though, to effectively tackling these issues is board awareness and support. If a school's board or governing body does not have someone accountable for data privacy and protection, the school is unlikely to provide the correct resources and support to overcome challenges like facial recognition.

# The Takeaway



**Awareness. Accountability. Management.** The right media management solution depends on the governance, policies, and culture of each school. Start by considering why photos and visual media matter to your school.

If visual media is integral to learning and communications, then a comprehensive solution must be considered that has the tools to protect user privacy while being able to manage and share visual media to benefit the entire school community.

## Guidelines for managing images:

- **Control Access:** Vidigami is an invitation-only system.
- **Informed Participation:** Vidigami's permission system gives users the ability to choose what is shared.
- **Document Consent:** Get consent from each parent / guardian and use Vidigami's consent management tools to ensure photos are being used in a way aligned to that consent.
- **Ability to revoke consent:** Each user has the ability within Vidigami to remove any photo from being shared.
- **Ensure accountability:** Only invited users with permission can upload and / or download from Vidigami. All uploaded media is tagged with the uploader's name.



# 8 Commonly Asked Questions

## 1. **Where does Vidigami store and process data it collects?**

The Vidigami service is hosted by Amazon AWS in data centers located in Canada, a country approved by the European Union (EU) and United Kingdom (UK) General Data Protection Regulation to provide adequate levels of data protection per GDPR requirements.

## 2. **How does Vidigami secure the data it collects?**

Vidigami is a private platform where authenticated access is required based on who your school invites. Each user has their own login and password once they've agreed to Vidigami's [terms of use](#). Each user is accountable for their actions within the Vidigami system.

Vidigami then protects the data stored in the system with encryption and a combination of anonymization techniques, such as pseudonymization and data recoding, to obfuscate user data.

## 3. **When is a photo considered biometric data?**

Biometric data is generally defined as data that captures unique physical characteristics that can be used to identify an individual. With respect to photos, some consider the photo itself to be biometric data. The more widely accepted interpretation is that **an image is not biometric data until it is used to create a model for automated facial recognition.**

According to the [UK Information Commissioner's Office](#), "photos are not automatically biometric data even if you use it for identification purposes. Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if you carry out "specific technical processing". Usually this involves using the image data to create an individual digital template or profile, which in turn you use for automated image matching and identification."

## 4. **Does Vidigami collect biometric data?**

Vidigami collects biometric data when information from a face tag is used to train facial recognition for automated face tagging.

## **5. May individual users withhold consent for face tagging or facial recognition?**

If a school opts in to use facial recognition, an individual user (student, parent, staff) may elect to withhold consent for their photo to be automatically tagged. In disabling facial recognition, the user may still be manually tagged but their data will not be used to train the system for automated recognition. If the user does not want to be tagged at all, they will need to withdraw or be deregistered in Vidigami.

Your school may also set preferences such as, whether parents may tag other students or whether students may tag staff and faculty. Vidigami provides multiple levels of user consent management so that schools are empowered with a platform that enables everyone to respect each other's privacy.

## **6. May a user request their data to be disposed?**

To support the principles behind the "right to be forgotten" or the "right for erasure", a user may request for their data in Vidigami to be removed. The removal of an individual's data involves a request to be "unregistered" or "opted out". By unregistering from Vidigami, the identity of the user is removed, and any images of the user would be untagged and anonymous. By opting out, the user remains in the system, but their tagged photos will be unshared with members of the community – regardless of who uploaded the photos.

## **7. May a user take their media with them before its disposed?**

Yes, if the school authorizes the ability for a user to download.

## **8. Is Vidigami responsible for data privacy regulation compliance?**

Vidigami provides the most robust solution for community photo management. Designed to serve the needs of schools, the system implements best practices related to protecting content rights and individual data privacy rights. This has enabled us to provide a solution that supports media literacy and citizenship education as it pertains to visual media as well as enable schools to enforce policies that honour the principles established by international data privacy laws, such as the General Data Privacy Regulation (GDPR) of the European Union (EU) and the United Kingdom (UK) for storing and sharing photos.

Given the changing landscape of data privacy law and regional interpretations, Vidigami cannot be responsible for regulation compliance. Please consult with your legal advisors to determine if Vidigami meets the needs of your school.