

Photos and Face Tagging

learn vidigami

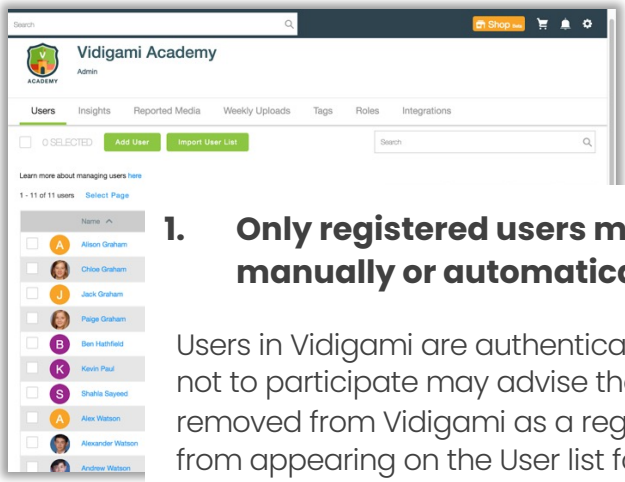
Photos, Face Tagging & Vidigami

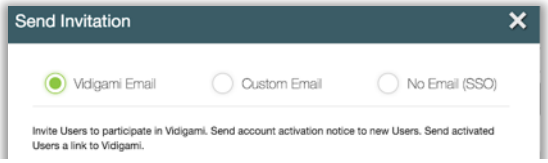
Thousands of photos and videos are captured every day from teachers, administrators, students, and families showcasing learning inside and outside the classroom. Tagging whether applied manually by users or automated by artificial intelligence (AI) helps organize content with valuable contextual information 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	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: 1. when a name is manually selected from the registered User list, or 2. when AI-enabled facial recognition technology matches a face to an individual.
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.

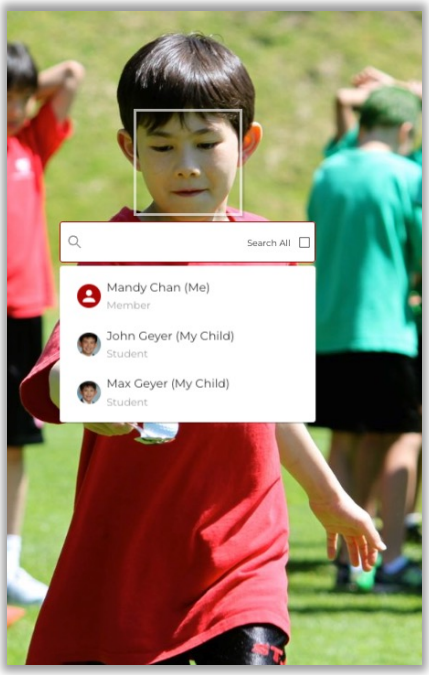
5 Things to Know About Tagging in Vidigami





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

Users in Vidigami are authenticated by their schools. 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 User 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.

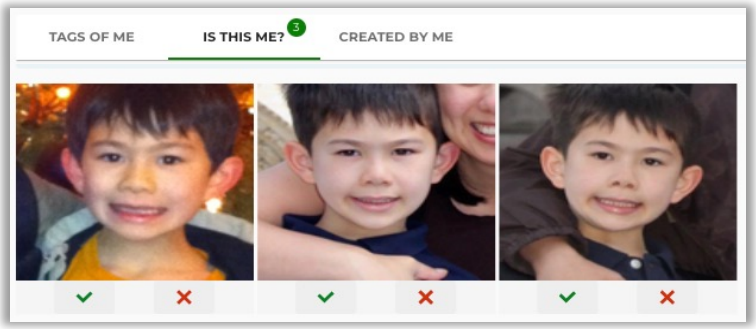
- **Automated Tagging:** The system leverages AI-enabled facial recognition to automatically generate face matches and tagging.
- **Assisted Tagging:** The system detects faces and prompts users to manually tag by selecting a name from the User list. When a face is not detected, the user may add a face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

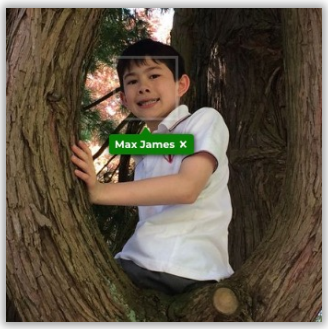
learn vidigami

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).

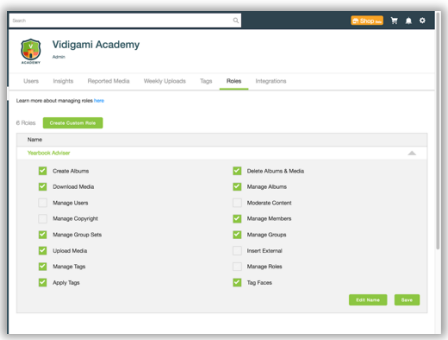
Manual recognition involves the verification of a detected face by an end user. The user will be able to select a name from the list added by the school. A user will not be able to be manually tagged if they are not in the user list in Vidigami.





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.



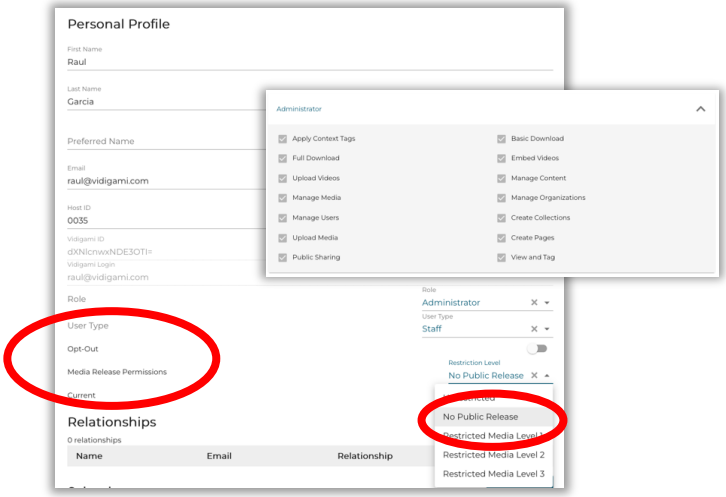
4. Organization permissions

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

By default, all users are given permission to tag themselves and their children. A school can choose to expand this permission to include the ability for 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 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 in Vidigami. Vidigami administrators can see each photo reported, the user who reported it, and the reason why.
- **Manual Tagging Only*** – A user or parent may elect for manual tagging only so that the system does not automatically match or tag their images. (*2023/24)



Weighing the value of facial recognition technology

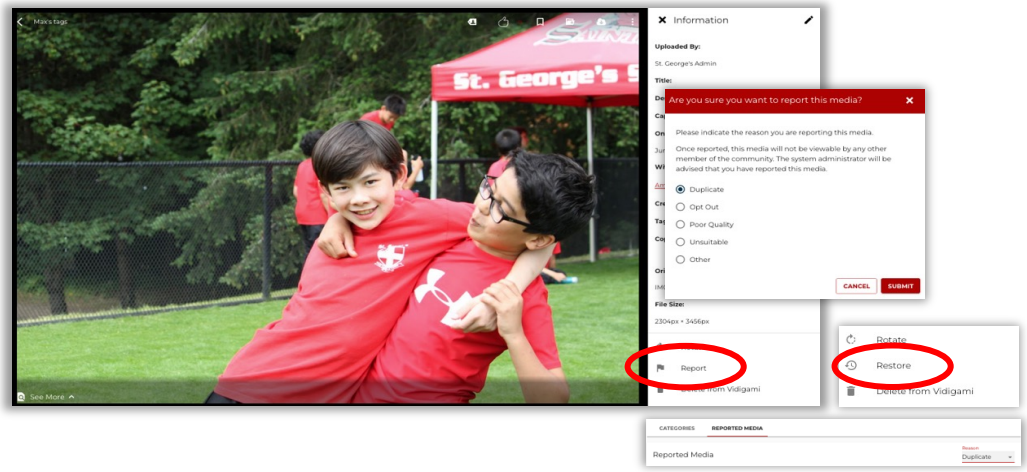
Each school must evaluate the risks and benefits of using facial recognition technology and decide what will work best for the school.

AI-enabled facial recognition leverages machine learning and biometric data to automate the process of identifying an individual and associating that individual with 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. Photos have become a universal language, integral to how we learn, how we teach and how we communicate. They are visually capturing learning inside and outside the classroom. They come from everyone. Everyone needs them for different reasons. Your photos are your stories. Consider why photos matter and the role they play in your school community.

Guidelines for managing images:

- **Control Access:** Participation is by invitation only.
- **Manage consent:** Ability to not only document user consent but to actively manage consent to ensure user rights are respected
- **Informed participation:** Users opt-in after understanding the options for how their content and images may be shared.
- **Ability to revoke consent:** Users are empowered to control how their images are shared, or not shared. That consent may be withdrawn at any time.
- **Ensure accountability:** Users are responsible for what they upload, download, or tag. Without anonymity, users can be self-governing.
- **Easily centralize. Intelligently organize. Automatically share.** A media asset management system that provides an efficient way of systematically organizing content and control over how that content is protected and shared within a school community.

learn vidigami

8 Frequently Asked Questions

1. Where does Vidigami store and process the 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. Does Vidigami collect biometric data?

Vidigami collects biometric data IF the school opts into using automated or manual tagging.

4. 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."

5. May individual users withhold consent for the collection of their biometric data?

If a school opts in to use facial recognition technology, individual users (students, families, staff) may elect to withhold consent for their photo to be automatically or manually tagged. A user or parent can request to be removed from the user list in Vidigami in which case there will be no automated, manual, or people tagging available for that user. In addition, a user can choose to allow manual and people tagging but request to be removed from the automated AI process of recognition.

Vidigami provides multiple levels of user consent management that empower users to restrict how their data is processed.

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

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 be "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, any photo tagged of the user will be unshared with members of the community.

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

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

8. Is Vidigami responsible for data privacy regulation compliance?

Vidigami provides the industry's leading solution for community photo management, designed with schools in mind. The system implements best practices related to protecting content rights and individual data privacy rights. This foundation supports media literacy and citizenship education as it pertains to visual media as well as enables 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 regulatory compliance. Please consult with your legal advisors to determine if Vidigami meets the needs of your school.