

Pixevely Notification Form



PARENT PRIVACY NOTIFICATION FORM SCHOOL MEDIA AND BIOMETRIC DATA PROCESSING

This privacy notice informs parents/legal guardians about how Nunawading Christian College processes personal data of its members (student/staff) through its digital media management system, Pixevely.

As part of the school's responsibility to provide a safe, organised, and well-functioning school environment, we have a legitimate interest in securely managing student photos. These images serve essential operational, administrative, and safeguarding purposes, including:

- Ensuring student safety by accurately identifying students for security and emergency procedures.
- Facilitating internal school functions such as yearbooks, class projects, and educational materials.
- Managing media consent preferences to ensure that photos are only used in accordance with guardian choices.
- Improving administrative efficiency by replacing scattered storage methods with a secure, privacy-first platform.

The school is aware that mishandling student photos, whether through accidental sharing, outdated permissions, or human error can compromise a child's security and privacy. The school is committed to ensuring the safety and security of student/staff images captured on school grounds and to safeguarding the broader school community.

The school collects and uses your child's personal information when they become a member, while they remain a member, and after they are no longer a member of the school. The school controls this personal data and is responsible for deciding how to hold and use this data in accordance with data protection law. The school does not share member data with any third parties except our contracted data processors, or, if it is agreed between staff/parent/student and the school's Administration team.

We process and store both personal data and sensitive personal data for media processing. Personal data includes member name (student, staff), parent/carer/guardian name, photos, photo location (if collected by original capture device and made only available to administration staff), parent email address. Sensitive personal data means "personal data resulting from specific technical processing related to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images...". The sensitive personal data we collect for school media processing is member face biometric data and it requires enhanced protection.

The legal basis that the school collects, uses and processes member biometric data in supporting its Media Management system is by consent.



- This Notification form sets out the purposes for the processing, and how your consent will be sought. This will be shared with you (staff) or your parent/carer/guardian (student) to obtain their consent.
- For the use of face matching technology to automatically apply consent on member photos stored in the school's media gallery, we will issue a consent form, and a manual copy when requested to do so by you or parent/carer/guardian.
- Strict controls will be applied to consent management of member images by default in the system and a 'do not publish' flag will be automatically applied until a face biometric consent form is submitted by member/parent/guardian/carer.
- In the event you withdraw consent, the school can switch off automated face matching for a member in its Gallery at any time and manually tag faces to continue to manage media consent. Such requests will result in that individual's biometric data being permanently deleted from the Gallery and their media consent will no longer be automatically applied in real-time.
- If you do not wish for your member's face information to be automatically processed by the school in their gallery, or your member (child) objects to such processing, the school will provide reasonable alternative arrangement which typically consist of staff manually identifying and tagging the member's face with their name, however, there will be a delay in applying their consent in the gallery and no guarantee that the member's face will be recognised and tagged in every image they are featured in.

The school will use member personal and sensitive data in its media management processing for a specific purpose only, which is to store in a single school-owned and controlled accessible and secure environment (Media Gallery), school media (i.e., namely photos and videos) related to members for the sole purpose of:

- 1) applying the member's consent in the school's Media Gallery, and
- 2) allowing the school to manage and search for images containing a member.

All such media will be stored in the school's Media Gallery hosted on the Pixevely platform in Australia. Access to the Media Gallery is controlled by the school and is by invitation-only. This enables the school to:

- Store and search pictures of events to which members are engaged in.
- Search and filter on member photo consent across all photos stored in the Media Gallery.
- Store and search videos of events where members are engaged and participate.
- Create an archive record collection where controlled access is assured and secure.
- Preserve records of historic value for the benefit of the school and its members.

Pixevely is an award-winning, ISO27001 certified (the internationally recognised standard for information security management systems) Australian-owned and based media management compliance service whose technical infrastructure is based in Australia. For further information about Pixevely's approach to privacy: [privacy-policy.pdf \(Pixevely.com\)](#).

Media management is an essential operational function in running our school, and managing consent of member images, at scale and in real-time, is necessary and proportionate for improving both our process efficiency and the safeguarding of our community, especially at-risk students and individuals. This processing is conducted in a manner that allows the

school to take timely and appropriate action to minimise risk and harm. We only collect member face biometric data for this sole purpose.



The school collects sensitive personal data of its members (encrypted face biometric data) during its media management processing so it can use Automated Face Recognition Technology (AFRT) to automatically detect and identify members in photos and automatically apply their photo consent to each photo hosted in the school's Media Gallery in real-time.

Facial recognition is a mathematical process that matches an individual's image (their face) with other images containing the same person. The stored biometric data is an encrypted mathematical algorithm of the member's face, kept separately from photos in an encrypted database, both at rest and in transit. Names are also stored in a separate, encrypted database, isolated from other personal data. All student data and biometric information are owned by the school and stored locally, protected by multiple layers of security. The algorithm is only readable within the Pixevety school system.

The school can assure you that a secure data protection process is in place to safeguard your data. The school designs, builds and runs its systems to make sure data is as safe as possible at every stage, both while it's processed and when it's stored. The school will not:

- Share or sell your member's personal data with any other third parties.
- Use analytic cookies on its media management platform. Pixevety will only use necessary cookies which enable the Gallery to function.
- Use member face biometric data for profiling, surveillance or automated decision-making.

The school:

- Will only share school media where you have provided the relevant consents.
- Will store all media in a school-owned private and secure local cloud service platform.
- May provide you with direct access to the Media Gallery or may choose to use the Pixevety platform as an internal admin tool only.
- May choose to use a controlled Pixevety shared collection link to securely publish media on its website and other publishing channels.
- Will ensure its Media Management platform provided by Pixevety has controlled access to apply security features and protections according to the administration of the service.

The school will only keep your personal data for as long as necessary for the purposes it has collected it for; the specific purpose of managing member media held in the school Media Gallery.

You can request member withdrawal from this processing at any time by communicating with the school.

The Pixevety platform is designed as a privacy-by-design compliance tool, allowing students and staff to opt out of face biometric data collection at any time. Upon opting out, all captured member biometric data is immediately and permanently deleted and the member's photo consent will no longer be automatically applied in real-time within the Media Gallery.

If you do not wish for your student's face to be automatically processed for recognition in the school's Media Gallery, or your child objects to such processing, the school will provide

reasonable alternative arrangements. This will typically consist of manually identifying and naming the student's face in the school Media Gallery, however, there will be a delay in consent application in the Gallery (i.e. identifying and applying consent to your child's photos), and there can be no guarantee that your child's face will be identified and tagged in every photo they are featured in.



If you have any questions about this privacy notice, please contact the privacy officer at the school who will provide advice and monitor the school's use of personal information: hop@nunawading.vic.edu.au (Julie, Head of Primary) or hos@nunawading.vic.edu.au (Hanna, Head of Secondary)

You can also contact The Office of the Australian Information Commission (OAIC) if you have questions. The OAIC is an independent regulator set up to uphold information rights by using [this form](#).