# Privacy Policy for Nelu

**Effective date:** April 12, 2026

**Last updated:** April 12, 2026

This Privacy Policy describes how **Nelu App** ("**Nelu**," "**we**," "**us**," or "**our**") collects, uses, discloses, stores, and protects personal information in connection with the Nelu childcare management application and related services. Nelu is designed for use by childcare centres, centre administrators, teachers, supervisors, parents, and guardians in Canada. The service is intended to support childcare operations, family communication, attendance tracking, daily reporting, room management, and controlled photo sharing.

Because Nelu handles information about children, families, and childcare staff, we treat this information as sensitive and aim to provide clear, specific disclosures. Canadian privacy guidance emphasizes that organizations should clearly explain what information is collected, why it is collected, who it is shared with, and what meaningful risks or consequences may follow from its use. Canadian privacy guidance also treats children's information as particularly sensitive and supports privacy-protective defaults for services involving children. [1] [2]

| Topic | Summary |
| --- | --- |
| **Primary use of the service** | Childcare administration, communication, attendance, reporting, and controlled photo sharing |
| **Primary hosting location** | Google Cloud Canada region in **Toronto** (`northamerica-northeast2`) as configured for core application data [3] |
| **Optional photo privacy feature** | Parent-controlled face matching and blurring workflow using AWS Rekognition, **off by default** [4] [5] |
| **Who provides child information** | Parents, guardians, and authorized childcare personnel; not children directly [2] |
| **Deletion requests** | May be submitted by email and handled through a documented verification and deletion workflow, subject to applicable legal, security, backup, contractual, or operational retention requirements [6] |

# 1. Scope and role of the service

Nelu is a platform used by childcare centres and families. Depending on the circumstances, **Nelu App** may act as a direct controller of certain account and service information, or as a service provider processing information on behalf of a childcare centre that uses the platform. Each childcare centre remains responsible for its own notices, consents, classroom practices, recordkeeping obligations, and legal compliance for how it uses the service in its operations.

Where a childcare centre provides its own privacy notice or parental consent forms, those centre-specific documents may apply in addition to this Privacy Policy. If there is a conflict between a centre’ s instructions and a feature configuration in the app, we may follow the centre’ s documented administrative instructions to the extent permitted by law and our contract with that centre.

# 2. Information we collect

We collect information that is necessary to provide, secure, maintain, and improve the childcare management service. This includes information provided directly by users, information generated through use of the platform, and limited technical information required for security and service operation.

| Category of information | Examples |
| --- | --- |
| **Account and identity information** | Name, email address, phone number if provided, login credentials or authentication identifiers, user role, and associated childcare centre |
| **Child profile information** | Child’ s name, date of birth, room assignment, allergies, dietary notes, authorized pickup contacts, medical or support notes entered by the centre or parent, and profile photo if used |
| **Parent and family information** | Parent or guardian names, contact details, emergency contacts, pickup permissions, and communications with the centre |
| **Staff and centre administration information** | Staff names, job roles, room assignments, supervisor designations, administrator permissions, and centre configuration settings |

| | |
|---|---|
| **Operational records** | Attendance, sign-in and sign-out records, daily reports, nap and meal logs, incident notes, activity updates, classroom posts, and related timestamps |
| **User content** | Messages, comments, attachments, photos, videos, and documents uploaded or shared through the app |
| **Optional face-processing information** | Images submitted for the optional face privacy feature, reference images or related face-matching inputs used to help blur or restrict sharing of a child’ s image, and related settings or consent status |
| **Technical and security information** | Device type, app version, IP address or approximate network information, log data, authentication events, and diagnostic information necessary to secure and operate the service |

We do **not** knowingly collect personal information directly from children through a child-facing interface. Information about a child is provided to Nelu by the child’ s parent, guardian, or authorized childcare personnel. Canadian privacy guidance states that organizations should make clear whether the parent or guardian, rather than the child, is providing consent and information for services involving children. 2

## 3. How we use personal information

We use personal information to operate the service, deliver requested features, administer childcare-centre access, protect the platform, respond to users, and meet legal obligations. We only use information for purposes that are reasonable in the childcare-management context and consistent with the service being provided.

| Purpose | Examples of use |
|---|---|
| **Provide the core service** | Creating and maintaining accounts, authenticating users, displaying classroom information, showing attendance and daily reports, and supporting family-centre communications |
| **Manage permissions and governance** | Applying role-based access controls, assigning rooms, limiting staff access, and enabling |

| | |
|---|---|
| | childcare administrators to configure teacher and supervisor permissions |
| **Support photo and media sharing** | Enabling users to upload, view, and share photos and videos within the app according to permissions and privacy settings |
| **Operate the optional face privacy feature** | Helping blur or restrict image visibility for a child when a parent or guardian has chosen to enable that privacy feature |
| **Security and integrity** | Monitoring misuse, enforcing access restrictions, maintaining logs, investigating incidents, and protecting accounts and infrastructure |
| **Customer support and service communications** | Responding to requests, sending administrative notices, and communicating changes affecting service use |
| **Legal and regulatory compliance** | Meeting applicable legal duties, responding to lawful requests, maintaining required business records, and enforcing contracts or policies |

We do **not** sell personal information. We do **not** use child, parent, or staff information for third-party advertising. We do **not** use the optional face privacy feature to make decisions about a child’ s eligibility, behaviour, or profile, and we do not offer it as a public facial recognition or surveillance tool.

## 4. Optional face privacy feature

Nelu offers an **optional** privacy feature intended to help parents or guardians limit how their child appears in shared group photos. This feature is **off by default**. A parent or guardian may choose to enable it for their own child if they want the app to help blur, mask, or otherwise limit the visibility of that child in certain shared images, or to apply child-specific visibility logic within the app.

This feature is designed as a privacy control, not as a general biometric identification system. When enabled, selected images may be processed to help identify the relevant child’ s face for privacy-related image handling. AWS Rekognition documentation distinguishes between non-storage image-analysis operations, in which input image bytes are not persisted, and storage-based collection features, such as face collections, that store mathematical face vectors. AWS also states in its public FAQ that image and video inputs

processed by Rekognition may be stored and used by AWS for limited service-related purposes unless the customer has configured the applicable opt-out controls. [4] [5]

> "Amazon Rekognition does not persist any information discovered about the input image. Like all other Amazon Rekognition API operations, no input image bytes are persisted by non-storage API operations." — AWS Rekognition Developer Guide [4]

> "Amazon Rekognition may store and use image and video inputs processed by the service solely to provide and maintain the service and, unless you opt out ... to improve and develop the quality of Amazon Rekognition..." — AWS Rekognition FAQ [5]

Accordingly, our intended design is that Nelu uses AWS Rekognition only for limited face-matching or image-analysis steps needed to support the optional privacy feature, and **we do not intentionally create or maintain searchable Rekognition face collections for children as part of the standard photo-blurring workflow unless expressly described elsewhere in centre documentation or feature settings**. However, because AWS acts as a third-party service provider, images or image data submitted to that service may be processed under AWS' s infrastructure and service terms. Parents or guardians who do not want this optional processing can simply leave the feature turned off.

If you enable this feature, you represent that you are the child' s parent or legal guardian, or that you otherwise have lawful authority to make that choice. If you disable the feature, we will stop using that child' s related face-processing setting for future supported photo-handling workflows, subject to reasonable technical processing time and any previously generated shared content already delivered within the service.

## 5. Consent, parental authority, and children' s privacy

Children' s personal information, including images and childcare records, is sensitive. Canadian privacy guidance states that organizations should use privacy-protective defaults, collect only what is necessary, provide meaningful and service-specific notice, and in most cases obtain parental or guardian consent for collection, use, and disclosure of personal information of children under 13. [1] [2]

For that reason, Nelu distinguishes between **core service processing** and **optional processing**. Core service processing includes the account, communication, attendance, reporting, and administrative functions needed for the childcare management service. Optional processing includes features such as the face privacy feature described above. When required, parents or guardians are responsible for deciding whether to enable optional child-specific features and for providing accurate authority and consent information.

If we learn that information was collected without appropriate authority, we may restrict processing, request additional confirmation, or delete the information where appropriate.

## 6. Where data is stored and processed

Core application data is configured to be stored in the **Google Cloud Canada region in Toronto**. Google's official locations documentation identifies Toronto as the `northamerica-northeast2` region. [3] We use cloud infrastructure and related service providers to host, secure, transmit, and process information necessary to operate the service.

Although our primary hosting configuration is in Canada, some limited processing, support, security, or service-provider operations may involve access from or processing in other jurisdictions depending on the tools enabled for the service, legal requirements, or provider operations. Canadian privacy guidance states that organizations remain accountable for personal information transferred to third-party processors, whether processing occurs in Canada or outside Canada. [7] For that reason, we require service providers to protect information using appropriate contractual, organizational, and technical safeguards.

| Infrastructure or processor context | Description |
| --- | --- |
| **Google Cloud Canada (Toronto)** | Primary hosting environment for core app data, including application storage and related infrastructure configured in the Canadian Toronto region [3] |
| **AWS Rekognition** | Optional processor used only when the parent-controlled face privacy feature is enabled and only for limited image-analysis functions tied to that feature [4] [5] |
| **Authorized childcare-centre administrators and staff** | May access information within the app based on assigned roles, rooms, and permissions |
| **Other service providers** | May support authentication, hosting, security, communications, or support functions where enabled and contractually authorized |

## 7. How we share information

We share personal information only where reasonably necessary to operate the service, follow childcare-centre instructions, protect rights and safety, or comply with law.

Information may be shared with the relevant childcare centre, its authorized administrators, teachers, supervisors, and staff based on assigned permissions and room access. Information may also be visible to parents or guardians where the app is configured

to provide family access to their child's classroom records, reports, messages, or shared media. Ontario childcare guidance emphasizes the importance of policies that explain who may access records and how family privacy is protected. [8]

We may also share information with infrastructure and service providers that help us host or operate Nelu, including Google Cloud and, where enabled, AWS Rekognition for the optional face privacy feature. We may disclose information where required to respond to lawful requests, protect the security of the service, investigate misuse, establish or defend legal claims, or enforce our agreements.

We do not disclose personal information to data brokers, and we do not permit third-party advertising networks to use childcare data from Nelu for targeted advertising.

## 8. Access controls, governance, and security

We use reasonable administrative, technical, and organizational safeguards designed to protect personal information against unauthorized access, loss, misuse, or disclosure. These safeguards may include authentication controls, role-based permissions, environment restrictions, encryption in transit and at rest where supported, security monitoring, logging, and internal access limitations.

Nelu uses a governance model in which childcare administrators can assign roles, rooms, and permissions to teachers, supervisors, and other authorized users. This design is intended to limit access to information according to the user's function in the childcare environment. Canadian privacy law and guidance do not require perfection, and no electronic system can be guaranteed to be completely secure. However, we take reasonable steps to reduce risk and to restrict access based on operational need. [10]

If you believe your account or a child's information has been accessed improperly, you should contact us immediately using the contact details below.

We maintain internal procedures for incident intake, containment, assessment, and response. Where required by applicable law, we may notify affected individuals, childcare centres, and regulators about breaches of security safeguards involving personal information. Canadian privacy guidance requires reporting and notification where a breach creates a real risk of significant harm, and it also requires organizations subject to PIPEDA to keep records of all such breaches. [1] [6]

## 9. Retention of information

We retain personal information only for as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer period is required or permitted by law, contract, dispute preservation needs, security needs, or childcare-centre recordkeeping obligations. Ontario childcare guidance recognizes that childcare records may be

maintained electronically and that centres should define privacy and access rules for those records. [8]

Retention periods may vary depending on the type of data, the instructions of the childcare centre, the status of the account, legal hold requirements, and the nature of the service function. Photos, daily reports, attendance records, messages, and child profile information may therefore remain available for the period needed to operate the service and meet applicable obligations.

Optional face privacy feature data will be retained only as long as reasonably necessary to provide that feature, unless earlier deleted or retention is required for a lawful reason.

## 10. Access, correction, and deletion requests

You may request access to, correction of, or deletion of personal information by emailing **privacy@neluapp.com**. If the request concerns a child, we may require confirmation that the requester is the child’ s parent, legal guardian, or otherwise authorized person. If the request is submitted through a childcare centre, we may coordinate with that centre before acting on the request.

Deletion requests are handled through an internal verification and deletion workflow. We may acknowledge the request, ask for identity or authority confirmation, clarify the scope of the request, consult the relevant childcare centre where appropriate, and then delete, de-identify, or restrict processing of information that we are not required to retain. We will review deletion requests and process them within a reasonable period, subject to identity verification, security needs, contractual obligations, legal requirements, dispute preservation, fraud prevention, backup retention cycles, and childcare-centre recordkeeping obligations. For that reason, we do **not** promise that every item of information can always be deleted immediately on demand. Where full deletion is not possible, we may instead restrict processing, archive required records securely, or explain what information must be retained and why. [9]

If you want all deletable data associated with your account or child profile removed, you may submit that request by email. We may ask for enough information to identify the relevant account, centre, child, and records. Deletion from active systems may occur before backup copies expire, and some backup copies may remain until the normal backup retention cycle ends where technically necessary.

## 11. External service providers

We use third-party service providers to support our operations. These providers may include cloud hosting providers, authentication providers, support tools, and limited image-analysis providers. When we transfer personal information to a service provider for

processing, Canadian privacy guidance states that we remain accountable for the information and must use contractual or other means to provide a comparable level of protection while it is being processed for us. 7

Where a service provider is involved in optional features, such as AWS Rekognition for the face privacy workflow, we aim to limit the information shared to what is reasonably necessary for that feature. We do not authorize service providers to use childcare data for unrelated marketing purposes on our behalf.

## 12. International and provincial legal considerations

Nelu is based in Canada and is designed for use in the Canadian childcare context, with an expected rollout beginning in Manitoba and expanding more broadly across Canada before any future expansion into other jurisdictions. Depending on where a childcare centre, parent, or staff member is located, different privacy laws may apply, including the federal **Personal Information Protection and Electronic Documents Act (PIPEDA)** or substantially similar provincial private-sector laws. This Privacy Policy is intended to support those frameworks, but it does not replace legal advice for childcare centres or families.

If Nelu is used in jurisdictions with additional requirements for minors, biometrics, education records, or childcare operations, users and centres are responsible for informing us of any special legal constraints that must be reflected in feature configuration or contract terms.

## 13. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in the law, the service, our providers, or our data practices. If we make material changes, we will post the revised version in the app or on the applicable website and update the effective date above. Where required, we will provide additional notice or obtain updated consent.

## 14. Contact us

If you have questions, concerns, or requests regarding privacy, children’ s information, or deletion, please contact:

**Nelu App**

**Privacy Contact:** Privacy Team

**Email:** privacy@neluapp.com

**Website:** neluapp.com

# References

[1] Office of the Privacy Commissioner of Canada - Guidelines for obtaining meaningful consent

[2] Office of the Privacy Commissioner of Canada - Tips for collecting personal information from kids

[3] Google Cloud - Locations

[4] AWS Rekognition Developer Guide - Storage and non-storage operations

[5] AWS Rekognition - Frequently Asked Questions

[6] Office of the Privacy Commissioner of Canada - What you need to know about mandatory reporting of breaches of security safeguards

[7] Office of the Privacy Commissioner of Canada - Guidelines for processing personal data across borders

[8] Ontario Child Care Centre Licensing Manual - Administrative matters

[9] Office of the Privacy Commissioner of Canada - Personal Information Retention and Disposal: Principles and Best Practices

[10] Office of the Privacy Commissioner of Canada - PIPEDA Fair Information Principle 7 – Safeguards