PRIVACY IMPACT ASSESSMENT (PIA)

Childcare Pro Children's Centre Management Software

A. GENERAL INFORMATION			
PIA File Number:	PIA-24-12		
Department/Faculty:	Education, Health, & Human Development		
Office/School:	Children's Centre		
Project Manager / PIA Drafter:	Trish O'Brien Robert Benedicto	**Title:**	
Email:	patriciaobrien@capilanou.ca robertbenedicto@capilanou.ca	**Phone:**	
Privacy Officer:	Jacquetta Goy – assessment completed by Isabel Melendez, Privacy, Information Access and Records Management Co-ordinator		
Email:	isabelmelendez@capilanou.ca	**Phone:**	[To be completed by the Privacy Officer]
Related PIAs, if any:	N/A		

1. Description of the Initiative:
To the best of your ability, please provide a detailed description of the initiative, its main objectives, the context in which it functions, the business need for it, and how the objective will meet that need.

The Children's Centre is currently managed by unsustainable, manual means. Employees transpose the majority of the information required for running the Children's Centre from incoming paper or electronic documents (applications and enrollment forms) into Excel sheets. They would like to eliminate the inefficient and paper-based system.

Childcare is a crucial component of the University's recruitment and retention strategy. Creating efficiencies will enable the Children's Centre to have accurate projections and allow them to maximize enrollment.

It is recommended that a Child Care Management system called ChildCare Pro be implemented. It is a standalone SaaS solution. All client data collected and stored will be from new accounts including CapU employees and students, etc. There will not be any

integration with Banner accounts. There is an option to integrate with CapU Outlook which would be desirable. SSO will be enabled for the Children's Centre admins.

2. Scope of this PIA:

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA? Describe what parts of the initiative you are assessing. If a project will be implemented in phases, be sure to explain which phase is being documented in the PIA. Subsequent updates or amendments can be made for other phases as they are developed

This PIA is limited to the use of the Childcare Pro childcare management software.

3. Elements of Personal Information:

To the best of your ability, please list all the data or information that will be collected, used, processed, stored, disclosed, or accessed as part of the initiative (not just the personal information). This will allow the Privacy Officer to assess all the information involved against what FIPPA considers to be personal information. For example, if conducting a survey, list the different elements of the information being collected as well as a summary of the other types of questions.

Family Information: Names, emails address, phone number, mailing address, Cultural/faith, Employer name and address, Copy of ID, Marital status/Custody orders/legal documents, Vehicle information for carpool parking.

Children's Information: Name, DOB, address, parent/guardian, siblings, Indigenous ancestry, medical alerts / medication to be given/care plans, Allergies, Vaccination history, Picture, Doctor and dentist, PHN, Birth certificate, People who are allowed to pick them up, Emergency contacts

Attendance records

Employee Information: Name, DOB, address, phone number, Indigenous ancestry, medical alerts, Allergies, Vaccination history, Picture, Doctor and dentist, PHN, Emergency contacts, License number for ECEs, First aid certification, Criminal Records Checks, Resume and cover letter and references.

4. Sensitive Personal Information:

	YES	NO
Will sensitive personal information be collected, stored, used, or disclosed as part of this initiative?	☒	☐
Will the sensitive personal information be stored outside of Canada? If so, please fill out Section E.	☐	☒

Sensitive personal information is not defined in FIPPA. Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used, or disclosed. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored.

Examples of sensitive personal information may include:

- *Personal health information*
- *Genetic and biometric data*
- *Personal financial information*
- *Geolocation data*
- *Criminal records*
- *Counselling records*
- *HR records*
- *Payroll records*

Please list sensitive personal information that will be collected and stored in this initiative:

Children's personal health information (PHN, Medical Alerts, Medication, Allergies, Vaccination Records, Doctor and dentist info, etc.)

Children's home addresses

Childcare Centre Staff addresses, licenses, and criminal record checks

Staff personal health information (Medical Alerts, Medication, Allergies, Vaccination Records, etc.)

B. COLLECTION & USE OF PERSONAL INFORMATION

1. Description (either a narrative or flow chart) of the linkages and flows of personal information collected, used, and/or disclosed:

Provide a step-by-step description from beginning to end showing how personal information is collected, circulated, processed, stored, and used, as part of this initiative, and if it is disclosed to any third parties. Please include all formats (paper and electronic) from creation or collection until final disposition. This can be demonstrated either via a flow chart, or a numbered list.

Receive information from applicants – inside or outside the university community

From that information specific reports for use on emergency cards, attendance sheets, etc. will be created.

Lists or reports to be available to classroom teachers only

Create report of emergency contact information and medical alerts that will stay in the office.

Staff information is to be entered into the system by staff members and available only to office staff who have specific permission.

The only time any information would be shared with anyone outside of office staff and classroom educators is if permission was given by the family to do so

PERSONAL INFORMATION FLOW TABLE:

	Description/Purpose	**Type** *(Collection, Use, Retention or Disclosure)*	**FIPPA Authority**
1.	Receive information from applicants.	Collection	Section 26
2.	Use information to determine student enrollment and student staff ratios.	Use	Section 32
4.	Information used by teachers for attendance, medical notes, pick up lists.	Use	Section 32
3.	Enrolled students' and staff's information goes into their files, emergency cards, etc.	Retention	Section 31

2. Collection Notification:
Will you be collecting personal information directly from the individual the information is about?
If so, please see below the sample of the collection notice you're required to provide.
Please indicate the location and placement of the notice (e.g., a form).

Example of collection notice:
"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information relates directly to and is necessary for an operating program or activity of the University. Questions about the collection of this information may be directed to the Privacy Officer at privacy@capilanou.ca".

Collection notice must be included clearly in onboarding paperwork/on the system so that guardians of incoming children and incoming student workers are aware of the collection authority and reasoning.

Please note that your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information is necessary for the operation of the Children's Centres. Questions about the collection of this information may be directed to Kelly Pickford, the Manager at the Children's Centre at kellypickford@capilanou.ca.

3. Direct / Indirect Collection (Section 27(1)):
If, for the purposes of the initiative, the personal information will only be collected directly from the individual the information is about, please identify when and where that collection will take place. If the initiative will collect personal information indirectly, (e.g., website cookies, public database) please provide details.

Personal information will be collected directly in a self-service portal when parents and/or Children's Centre staff input information regarding their children. This includes information about health needs, authorized contacts, etc. The other case of direct collection is staff entering information related to day-to-day activities such as attendance and wellbeing. There will not be any information included about children's performance or behavior.

4. Authorization for Collection (Section 26):
Please describe why it is necessary to collect personal information, in order to fulfill the identified purpose(s) of the initiative. The collection of personal information should be limited only to those information items that are strictly necessary.

It is required to collect the children's family's addresses, contact information, emergency contacts, children's identification information, health profile etc. to ensure the safety of the children enrolled in the Children's Centre.

5. Authorization for Use (Section 32):
List the uses of personal information:

Email parents about things happening at the Centre
Mail parents refund cheques, or perhaps hard copies of receipts for childcare fees if requested
Ensure that children are not given food to which they are allergic
Know the doctor or dentist information in case of emergency
Know who to call in case of emergency, and know the care plan if required
Phone the parents if the child is unwell
Ensure that only people authorized to pick up children do so

Please respond to the following statements:	YES	NO
Will the information be used only for the purpose(s) for which it was obtained?	☒	☐
To prevent the use of collected personal information for secondary purposes, safeguards are /will be in place on access to both electronic and hard copies.	☒	☐
Will data be anonymized or aggregated at any point for planning or reporting purposes?	☒	☐

Data about the number of children enrolled into the Childcare Centre will be shared with the provincial government.

6. Marketing Uses:
Please identify any anticipated uses of personal information for marketing purposes. All marketing via commercial electronic message (email, text message, etc.) must comply with the rules of Canada's Anti-Spam Law (CASL). All marketing via telephone must comply with the National Do Not Call List (DNCL) Rules.

None of the information collected and/or stored in this system will be used for marketing.

C. ACCESS, DISCLOSURE & STORAGE OF PERSONAL INFORMATION

1. Access to Personal Information:

Identify who will have access to personal information as a result of this project (e.g., teams, roles, or individuals, including any third party service providers, contractors, etc.), what type of personal information will they be privy to, the purposes for which they will have access, and how information will be made available to them/user access assigned?

Who?	Type of PI?	Purpose(s)?	How?
Children's Centre Director and Manager	Higher levels of permissions	Setting up and administering profiles, safety of the children	Parents will give permission when they choose to enter their personal information
Children's Centre Office Assistant	Higher levels of permissions	Setting up and administering profiles, safety of the children	Parents will give permission when they choose to enter their personal information
Children's Centre Educators	Minimal viewing/editing	Entering attendance info, confirming pickups/drop offs, checking medication/allergies	Childcare Pro or Bri, Sara and I will ensure the settings in the system give access to only the information that the educators need
Parents/Guardians	Minimal viewing/editing	Filling out and updating children's profiles	Childcare Pro will ensure the settings allow the parents and guardians to see only their own personal information

Please respond to the following statements:	YES	NO	N/A
Access to personal information is based on a need-to-know basis.	☒	☐	☐
If you're utilizing third party for storage/processing of personal information, do you have controls in place to monitor access?	☒	☐	☐
Is there an ongoing audit process that can track access (e.g., who accessed and/or updated personal information records and when)?	☒	☐	☐

Provide details about how you will track and monitor access to personal information (e.g., audit trails or physical sign-in and sign-out of files)?

People's accounts are password protected; The system currently does not have the ability to pull audit reports digitally. A system will be put in place to verify on a regular basis that only the authorized people have access.
Is there a defined approval process in place for granting access? Is there a person (title) who will authorize and/or revoke access? How/how often will the approval authorities be reviewed to ensure they are current?
Children's centre administrators will have the power to approve/deny who gets access.
Identify who (title) has the authority to add, change or delete personal information. Is this power limited to a specific individual(s) or anyone with access can add, change, or delete personal information?
Children's Centre Director, Manager, and Office Assistants will have more permissions, parents will have limited access to their children's info/profile, other Children's Centre staff will be able to view class info and update attendance records.
What controls are in place to prevent unauthorized access to personal information (e.g., locked cabinets, key cards, passwords)?
The system requires user authorization and passwords. The system has cybersecurity protection controls in place such as encryption, firewall, etc. Computers in the Children's Centre where the system is accessed are located in locked rooms that require key cards for opening the doors.
If there is a third party or a service provider involved in the initiative, what access controls are/will be put in place?
ChildcarePro is the third party offering ChildcarePro software and cloud storage. They have policy and training in place to reduce PI related risk. Furthermore, they will not be handling system migration but allowing CapU the tools to complete the migration ourselves.

2. Disclosure of Personal Information:			
Please respond to the following statements:	**YES**	**NO**	**N/A**
Will personal information be disclosed internally to an employee, only when the information is necessary for the performance of the duties of that employee?	☒	☐	☐
Will the personal information be disclosed externally to a service provider, only when the information is necessary for the delivery of the contracted services?	☐	☒	☐

3. Storage of Personal Information: *Describe exactly where and how will the personal information be stored.*	
WHERE? *e.g., in Canada or outside Canada? Provide details.*	Cloud storage based in Canada

HOW/WHAT FORMAT? *e.g., electronic, and on-premise servers or data centres.*	Electronic cloud storage

D. ACCURACY, CORRECTION, RETENTION & DISPOSAL OF PERSONAL INFORMATION

1. Decisions Affecting Individuals (Section 28):

	YES	NO
As part of this initiative, an individual's personal information will be used to make a decision that directly affects the individual.	☒	☐

Examples of using personal information to make decisions include but are not limited to:

- *Using a person's employment history to decide whether they can move forward in a job competition*
- *Using a student's exam results to pass them in a course*
- *Using a student's information to approve them for financial aid*

If "yes", please explain how and why that will be done:

Personal information about the child will be used in order to provide the best care for them.

If employees input personal information into the system about their health, that will be collected and stored in this system, but it will only be used to ensure that they get appropriate medical attention if required.

If answered "yes" above, please respond to the following statement:

Public bodies are required to keep personal information for a minimum of one year after it is used to make a decision that affects the individual.
Please describe how/what steps will be taken to ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

Information must be kept for seven years after a student leaves the program. The files will be kept in the Childcare Pro system for the required amount of time before they are deleted.

2. Accuracy of Personal Information (Section 28):
If an individual's personal information is used to make a decision that directly affects that individual, please explain the efforts that will be made to ensure that the personal information is accurate and complete (e.g., collecting the information directly from the individual, verifying the information with the individual prior to recording it, etc.).

Information will be collected directly from the individual (in the case of staff) or their guardian (if they are children) and will be regularly verified on an annual basis.

3. Correction of Personal Information (Section 29):
Please describe how an individual can update or correct their personal information. Describe the process, this could be processes where an individual can ask for system administrators to make changes on their behalf.

Corrections will be available via Self-service portal or can be done by Children's Centre staff.

If it is not possible to update or correct the information (for physical, procedural, or other reasons) please explain how it will be annotated to reflect that the correction was requested but not made.

In the unlikely case that information cannot be corrected, notes will be made on the child or Children's center employee's file.

Where personal information is disclosed to third parties, how will the third parties be notified of the update, correction, or annotation?

There will not be any disclosure of information to a third party. The agreement with the service provider includes a section on personal information. In this section, they will restrict unauthorized access, disclosure, use, copying of any PI in the system.

To be completed by the Privacy Officer:

s. 29	Right to request correction of personal information	**YES**	**NO**	**N/A**
	Are there procedures in place to enable an individual to request/review a copy of their own personal information?	☒	☐	☐
(1), (2)	Are there procedures in place to correct or annotate an individual's personal information if requested, including the source that was used to update the file?	☐	☐	☒
(3)	Is there a process in place to notify third parties where a correction is requested?	☐	☐	☒
	Do controls and procedures exist for the authority to add, change, or delete personal information?	☒	☐	☐
	Are reasonable efforts taken to ensure that personal information is accurate and complete if being used to make a decision that directly affects the individual?	☒	☐	☐

4. Records Retention (Section 31):

Personal information collected, used, and/or disclosed as part of this initiative must have an assigned retention period. Is there a defined retention period assigned? How long the records will be retained for?

After children leave or graduate from the Children's Centre, Vancouver Coastal Health requires a 7-year retention before records can be destroyed.

5. Disposal

How are the records containing personal information disposed of?
Who (title) is in charge of disposing them?

Children's centre administrators would be in charge of disposal. It is currently unknown if the ChildcarePro system provides disposition alerts. Currently, disposal is handled manually. With regular checks to see which files have completed their retention periods.

E. ACCESS, DISCLOSURE, STORAGE, RETENTION & DISPOSAL OF SENSITIVE PERSONAL

INFORMATION OUTSIDE OF CANADA

Complete this section only if you are disclosing or storing sensitive personal information outside of Canada. Please contact the Privacy Officer for assistance.

To be completed by the Privacy Officer:		
	YES	NO
Is it necessary to fill out section E. of this PIA?	☐	☒

F. RISK MANAGEMENT & SECURITY OF PERSONAL INFORMATION

1. Protection of Personal Information (Section 30):
Describe the audit, compliance, and enforcement mechanisms in place to protect against the unauthorized collection, access, use, disclosure, or storage of personal information, in course of the initiative (including for contracted service providers).

Children's Centre staff receive the CapU Privacy Protection training, Regular criminal record checks every 3 years. They are subject to the University's privacy policy and ensure that only authorized staff have access to children's PI in the ChildcarePro system.

2. Policies and Procedures:
Are there policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information? How will these be communicated to necessary parties, including employees, contractors, and third party service providers?

B.604 Acceptable Use and Security of Digital Technology Policy

B.700 Privacy and Access to Information Policy

B.700.1 Personal Information Incident Management Procedure

Children's Centre Operations Manual

3. Training:
Please describe how the conditions detailed in this PIA will be communicated to necessary parties, including employees, contractors, and third party service providers? Will specific guidance or training be provided on how to handle personal information in a privacy protective manner? Where you rely on enterprise-led privacy awareness training alone, please indicate this.

Children's Centre staff receive CapU privacy training and some privacy related training within the process of getting licensed by the Ministry of Education and Childcare. ChildCarePro staff are subject to their own privacy training and policies, on top of their other protections.

4. Privacy Incident Reporting:
Please describe how necessary parties, including employees, contractors, and third party service providers, will be made aware of the privacy incident notification process (as documented in the University's "Personal Information Incident Management Procedure").

Privacy Incident reporting in the Children's Centre aligns with B.700 Privacy and Access to Information Policy and B.700.1 Personal Information Incident Management Procedure.

5. Contract:

Has there been a contract drafted or signed? If so, please indicate below and provide a copy to the Privacy Officer.

A service agreement is saved with this PIA.

6. Contractual Privacy Provisions:

If the contract has been drafted or signed, does it include privacy provisions?

The service agreement has privacy provisions limiting unauthorized access, use, or disclosure to CapU's system and information. It also details the use of encryption and firewalls to secure all data in ChildcarePro.

7. Risk Reduction:

How will you (and the third party providers, if applicable) reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- *Destroy it*
- *Return it*
- *Transfer it to the correct recipient*

Parents will be provided with limited options to enter information into the system. In the event that PI is unintentionally collected, that information will be deleted from the system as soon as it is identified or during routine cleanup of records in the system.

8. Digital Tools, Databases, or Information Systems:

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats.

	YES	NO
Does your initiative involve digital tools, databases, or information systems?	☒	☐

If "yes", please describe:

The entire Management System will be a digital database. It will be noted as one of the University's personal information banks.

To be completed by the Privacy Officer:

9. STRA (Security Threat and Risk Assessment):

Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses. If a security assessment will be completed during the development of the initiative, the questions about technical security in this PIA template do not need to be completed. Instead, once the assessment has been finished it should be attached to the template.

	YES	NO
Will a separate security assessment be completed?	☒	☐

If "yes", please describe the assessment to be undertaken, including who will complete the assessment and when it will be completed:

28-Jan-2025: Michael Shi completed the STRA and approved the system.

10. Physical Security Measures:

Please describe the physical security measures established to protect the personal information in all media forms from unauthorized access. *Describe all aspects of the physical environment where personal information is held (e.g., Server(s) location/security, key card access to offices, CCTV surveillance, shredding, locked cabinets, password encryption for computers/laptops, alarm systems, building protection, staff screening, onsite security personnel, etc.).*
Computers in the Children's Centre where the system is accessed are located in rooms with multiple physical security measures. Some of the measures included are locked doors, CCTV surveillance, staff screening, and onsite security personnel.

To be completed by the Privacy Officer:		
	YES	**NO**
Is there reasonable technical security in place to protect against unauthorized access or disclosure?	☒	☐
Is there reasonable physical security in place to protect against unauthorized access or disclosure?	☒	☐
Comments: This system currently does not have internal auditing capabilities; however, the tools are currently in development.		

To be completed by the Privacy Officer:		
11. a) Data-linking Initiative:		
Please respond to the following statements:	**YES**	**NO**
Personal information from one database will be linked or combined with personal information from another database.	☐	☒
The purpose for the linkage is different from that for which the personal information in each database was originally obtained or compiled.	☐	☒
Data linking will occur between either (i) two or more public bodies or (ii) one or more public bodies and one or more agencies.	☐	☒
11. b) Based on the answers above, is this initiative a data-linking program under FIPPA (? *If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.*		
This initiative is not a data-linking initiative.		

To be completed by the Privacy Officer:		
12. a) Common or Integrated Program or Activity:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves a program or activity that provides a service (or services) to the public.	☒	☐

Those services will be provided through (i) a public body and at least one other public body or agency working collaboratively to provide that service or (ii) one public body working on behalf of one or more other public bodies or agencies.	☒	☐
There is a written agreement signed by the head of each public body and agency through which the services of the program or activity are provided.	☒	☐
12. b) Based on the answers above, is this initiative a common or integrated program or activity? *Under section FIPPA 69(5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.*		
This initiative is a common or integrated program and will be submitted to the OIPC.		

To be completed by the Privacy Officer:		
13. a) Project with High Visibility/Public Interest, and/or Audio/Video Surveillance:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves installation or use of audio recording equipment.	☐	☒
This initiative involves installation or use of video recording equipment.	☐	☒
This initiative involves the use of new technology which might be perceived as being privacy intrusive. For example, the use of biometrics or facial recognition.	☐	☒
This initiative involves a program or activity that may generate high visibility or public interest.	☐	☒
13. b) Based on the answers above, does this initiative qualify as a project with high visibility/public interest, and/or does it include audio or video surveillance? *If so, the completed PIA should be sent to the OIPC for review and comment.*		
This will not be an initiative with high visibility or public interest.		

To be completed by the Privacy Officer:
14. Privacy Risks: *Use the table below to outline the risk associated with unauthorized collection, use, disclosure, or storage of personal information. Include a description of the potential impacts (consider both individuals and any broader impact if relevant) and then rate the likelihood and the level of risk (use a simple low, medium & high scale). For each privacy risk identified describe the current controls and those that will be put in place as part of the initiative. Controls may include contractual, technical, security, administrative and/or policy measures. Where the level of risk is still significant describe the additional controls that need to be implemented.*

Area of Risk Exposure	Likelihood	Impact	Level of Privacy Risk	Mitigation Strategy / Actions	Responsibility for Mitigation Actions	Timeline for Mitigation Actions
Unauthorized employees or individuals could access the personal information in the system and use or disclose it for personal purposes	Low	High	Med	Employee code of conduct, privacy policy, VCH regulations are in place to prevent unauthorized use of PI. Access to system requires credentials and password. Computers with access to system will be in locked rooms.	Children's Centre Staff	Ongoing Mitigation – Prevention before breaches; any breaches will be responded to immediately following University procedure.
Unauthorized individuals at ChildcarePro could access PI	Low	High	Med	Employees of ChildcarePro are required to act in a manner consistent with their privacy policy and client agreement. Furthermore, they will not have access to CapU PI without consent and monitoring of program area administrators.	Children's centre Staff ChildcarePro Staff	Ongoing mitigation
User's PI is compromised during transmission.	Low	Med	Low	Digital security measures such as encryption, threat detection, etc. in use	ChildcarePro developers.	Ongoing mitigation

G. PERSONAL INFORMATION BANKS & INFORMATION SHARING AGREEMENTS

To be completed by the Privacy Officer:

1. Personal Information Bank (PIB)

PIB is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned only to that individual. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- *Linked to an identifiable individual*
- *Organized and capable of being retrieved by a personal identifier*
- *Normally compiled for a single purpose*

	YES	NO
Will this initiative result in the creation of a personal information bank?	☒	☐

If "yes", fill in the table below:

Describe the type of information in the bank:	The bank will include personal information about children, contact information for their guardians, staff personal information, and personal health information.
List any other ministries, agencies, public bodies, or organizations involved:	There will not be any other institutions involved with the PIB.
Record the Business contact title and phone number for person responsible for managing the PIB:	Children's Centre Director Sara Sutherland sarasutherland@capilanou.ca

To be completed by the Privacy Officer:

2. Information Sharing Agreements (ISAs) & Systematic or Repetitious Disclosure/Exchanges

Public bodies enter Information Sharing Agreements (ISAs) when there is a regular and systematic exchange of personal information between public sector organizations or between a public sector organization and an external agency. ISAs document the terms and conditions of the exchange of personal information in compliance with the provisions of the Act and any other applicable legislation. ISAs help to ensure privacy protection where personal information is exchanged.

	YES	NO
Does this initiative involve an Information Sharing Agreement?	☐	☒
Is the ISA added as an appendix to this PIA?	☐	☒

To be completed by the Privacy Officer:

	YES	NO
Does the initiative involve a regular and systematic exchange of personal information on a regular or ongoing basis between public bodies and/or external agency(ies)?	☐	☒

If "yes", please explain.
For example: the initiative will involve systematic collection and disclosure of personal information, in order for the department to provide specific services to students.

n/a

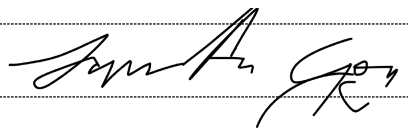
H. SIGNATURES

Project Manager Signature:

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used,

stored, or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.	
Title:	**Children's Centre Director**
Name:	**Sara Sutherland**
Date:	
Signature:	

Privacy Officer Comments & Signature:	
Comments:	This system has sufficient digital, physical, and personal protections in place to protect the user's and children's PI.
Name:	**Isabel Melendez**
Date:	**24 March 2025**
Signature:	

Additional Signatures (if required):	
Title:	Director, Risk Management and Privacy Officer
Name:	Jacquetta Goy
Date:	
Signature:	

This PIA received final review and approval in April 2026

I. APPENDICES		
	YES	**NO**
Will this PIA include appendices?	☒	☐
If "yes", please list them, and combine them with the PDF of this PIA. *For example: excerpt from a contract/privacy schedule, third party provider policies, blank questionnaire/examples of PI being collected during the course of the initiative.*		
Service Agreement		

Notice