



Outside of School Hours Care Confidentiality and Recordkeeping Policy

Aim:	This policy will provide guidelines for Pomonal Primary Outside of School Hours Care (OSHC) to ensure compliance with privacy and information management legislation for the collection, storage, security, use, disclosure and disposal of personal information, including photos, videos and health information.
Date of Operation:	12/07/2021
Review Dates:	October 2023

POLICY

Pomonal Primary OSHC is obligated by law, service agreements and licensing requirements to comply with the privacy and health records and information management (record-keeping) legislation when collecting personal and health information about individuals. The Health Records Act 2001 (Part 1, 7.1) and the Privacy and Data Protection Act 2014 (Vic) (Part 1, 6 (1)) include a clause that overrides the requirements of these Acts if they conflict with other Acts or Regulations already in place. For example, if there is a requirement under the Education and Care Services National Law Act 2010 (National Law) or the Education and Care Services National Regulations 2011 (National Regulations) that is inconsistent with the requirements of the privacy legislation, services are required to abide by the National Law and National Regulations. The Pomonal Primary OSHC service will understand and meet requirements for creating, storing and disposing of OSHC records.

Pomonal Primary school council is responsible for:

- Ensuring all records and documents are maintained and stored in accordance with Regulations 181 and 183 of the National Regulations (Refer to **Appendix 1: Definitions**)
- Ensuring the service complies with the requirements of the Privacy Principles as outlined in the Health Records Act 2001, the Privacy and Data Protection Act 2014 (Vic) and, where applicable, the Privacy Act 1988 (Cth) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), by developing, reviewing and implementing processes and practices that identify:
 - What information the service collects about individuals, and the source of the information
 - Why and how the service collects, uses and discloses the information
 - Who will have access to information
 - Risks in relation to the collection, storage, use, disclosure, or disposal of and access to personal and health information collected by the service

- Providing adequate and appropriate secure storage for personal information collected by the service, including electronic storage
- Developing procedures that will protect personal information from unauthorised access, including data integrity strategy
- Developing procedures to monitor compliance with the requirements of this policy
- Ensuring all employees and volunteers are provided with a copy of this policy, including the Privacy Statement of the service.

The Nominated Supervisor is responsible for:

- Ensuring they are aware of their responsibilities in relation to the collection, storage, use, disclosure and disposal of personal and health information in accordance with relevant legislations including, the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS)
- Ensuring families and carers know why relevant information is being collected, how it will be stored and reasons that it might be disclosed to other authorised services
- Ensuring the appropriate use of images of children, including being aware of cultural sensitivities and the need for some images to be treated with special care
- Ensuring all employees and volunteers are provided with a copy of this policy, including the Privacy Statement of the service
- Ensuring all families and carers are provided with the service's Privacy Statement and all relevant forms
- Informing families and carers that a copy of this policy is available on request
- Ensuring a copy of this policy is prominently displayed at the service and available on request
- Establishing procedures to be implemented if families and carers request that their child's image is not to be taken, published, or recorded, or when a child requests that their photo not be taken.
- Providing notice to children and families and carers when photos/video recordings are going to be taken at the service
- Ensuring educators and all staff have read and understood this policy and are aware of how to access it
- Obtaining informed and voluntary consent of the families and carers of children who will be photographed or videoed.

Educators are responsible for:

- Recording information on children, which must be kept secure and may be requested and viewed by the child's families and carers and representatives of the Department of Education and Training during an inspection visit
- Ensuring they are aware of their responsibilities in relation to the collection, storage, use, disclosure, and disposal of personal and health information in accordance with relevant legislations including the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS)
- Implementing the requirements for the handling of personal and health information, as set out in this policy
- Respecting family and carer choices about their child being photographed or videoed, and children's choices about being photographed or videoed.

Record Keeping

Pomonal Primary OSHC service will be responsible for creating, managing, and appropriately disposing of records in accordance with Education and Care Regulations, Family Tax Law and Public Records Act 1973 (Vic)(refer to **Appendix 2**: Summary of record keeping periods).

Record storage

All records must be kept in a safe and secure place only accessible by approved personnel. Written records include records that are made and stored electronically, as long as they are stored safely and any changes, apart from incidental changes related to their storage and display, are also recorded.

Records storage and access

Pomonal Primary OSHC will refer to the school's systems and processes for managing electronic and hardcopy records to ensure the authenticity, security, reliability and accessibility of these records.

All records will be stored in safe and secure locations to ensure their integrity and accessibility.

Information security and data integrity

OSHC services and schools must protect the confidentiality, integrity and availability of school information. They will manage and share information appropriately and securely in order to meet information security obligations and to appropriately protect staff, students and their families. The service will comply with the Department of Education and Training InfoSafe Policy and Guide (refer to **Appendix 3**: Information security and data integrity).

Legislation, Standards and Provisions

- [Education and Care Services National Law Act 2010](#)
- [Education and Care Services National Regulations 2011](#)
- [A New Tax System \(Family Assistance\) \(Administration\) Act 1999](#)
- [A New Tax System \(Family Assistance\) Act 1999](#)
- [Family Law Act 1975](#)
- [Children, Youth and Families Act 2005 \(Vic\)](#)
- [Child Care Subsidy Secretary's Rules 2017 \(legislation.gov.au\)](#)
- [Child Safe Standards](#)
- [Child Wellbeing and Safety <https://www.legislation.vic.gov.au/in-force/acts/child-wellbeing-and-safety-act-2005/031> Act 2005 \(Vic\)](#)
- [Child Wellbeing and Safety \(Information Sharing\) Regulations 2018](#)
- [National Quality Standard, Quality Area 7 – Governance and Leadership](#)
- [Equal Opportunity Act 2010 \(Vic\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Privacy and Data Protection Act 2014 \(Vic\)](#)
- [Accident Compensation \(OHS\) Act 1996 \(Vic\)](#)
- [Crimes Act 1958 \(Vic\)](#)
- [Education and Training Reform Act 2006 \(Vic\)](#)
- [Equal Opportunity Act 2010 \(Vic\)](#)
- [Evidence Act 2008 \(Vic\)](#)
- [Family Violence Protection Act 2008 \(Vic\)](#)
- [Family Violence Protection \(Information Sharing and Risk Management\) Regulations 2018 \(Vic\)](#)
- [Family Violence Information Sharing Scheme](#)
- [Financial Management Act 1994 \(Vic\)](#)
- [Freedom of Information Act 1982 \(Vic\)](#)

- [Health Records Act 2001 \(Vic\)](#)
- [Public Administration Act 2004 \(Vic\)](#)
- [Public Records Act 1973 \(Vic\)](#)
- [My Time, Our Place](#)
- [Child Information Sharing Scheme](#)
- [Victorian Data Sharing Act 2017 \(Vic\)](#)

Supporting Documents

- **[Department Education and Training \(DET\) - School Operations](#)**
[Department Education and Training: School Council](#)
[Department Education and Training: Information Security, InfoSafe](#)
[Department Education and Training: Records Management](#)
- **[Department Education and Training \(DET\) - Human Resources](#)**
[Department Education and Training: Conflict of Interest](#)
[Department Education and Training: Report Fraud or Corruption](#)
[Information Security for School Staff e-learning module](#) (Login required)
- **Australian Children's Education and Care Quality Authority (ACECQA)**
[ACECQA National Quality Standard](#)
[National Quality Agenda IT System](#)
- **[Australian Government](#) Department Education, Skills and Employment (DESE)**
[Child Care Provider Handbook - Child Care Subsidy System 2019](#)
[Child Care Subsidy - Specified Personnel Roles](#)
[Child Care Subsidy - Fit and Proper Requirements Personnel](#)
[Child Care - Financial Integrity](#)
- **Australian Government – Human Services**
[Australian Government – Service Australia – PRODA Login](#)
- **Australian Cyber Security Centre**
<https://www.cyber.gov.au/>
- **[Australian Competition and Consumer Commission](#)**
[Sign up for newsletter: https://www.scamwatch.gov.au/](#)

Roles and Responsibilities

Department/Role	Responsibility
Educators and Supervisors	Educators, Supervisors, Nominated Supervisor/Educational Leader will oversee the implementation and service adherence to this policy All Educators are responsible for the daily implementation of the policy when directly supervising children.
School Council / Principal	Provider official sign off on the Policy

Policy Review

The Policy will be reviewed every 12 months. The ongoing monitoring and compliance to this policy will be overseen by Nominated Supervisor, Pomonal Primary OSHC and Person with Management or Control of the Service where practical. Feedback from Quality Assessment and Regulation Division (QARD), received through the assessment and rating process and/or compliance visits will inform this policy review. Feedback from Department Education, Skills and Employment (DESE), stakeholders, e.g., families and carers, school community etc. will also inform policy updates and review.

Legislation, Standards, and Provisions

- [Education and Care Services National Law Act 2010](#)
- [Education and Care Services National Regulations 2011](#)
- [A New Tax System \(Family Assistance\) \(Administration\) Act 1999](#)
- [A New Tax System \(Family Assistance\) Act 1999](#)
- [Family Law Act 1975](#)
- [Child Care Subsidy Secretary's Rules 2017 \(legislation.gov.au\)](#)
- [Child Safe Standards](#)
- [National Quality Standard, Quality Area 5 – Relationships with Children](#)
- [National Quality Standard, Quality Area 6 – Collaborative Partnerships with Families and Communities](#)
- [Equal Opportunity Act 2010 \(Vic\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Privacy and Data Protection Act 2014 \(Vic\)](#)
- [Child Safe Standards](#)

Supporting Documents

- [Department Education and Training \(DET\) - School Operations](#)
[Department Education and Training: Information Security, InfoSafe](#)
- [Australian Children's Education and Care Quality Authority \(ACECQA\)](#)
[ACECQA National Quality Standard](#)
[National Quality Agenda IT System](#)
- [Australian Government](#) Department Education, Skills and Employment (DESE)
[Child Care Provider Handbook - Child Care Subsidy System 2019](#)

Acknowledgement

I acknowledge:

- receiving the Pomonal Primary OSHC Confidentiality and Recordkeeping Policy;
- that I will comply with the policy; and
- that dependent on the seriousness of any breach there may be disciplinary consequences if I fail to comply, which may result in the termination of my employment.

Your Name:	Belinda Wethers
Signed:	
Date:	05/11/22
Pomonal Primary School OSHC sign off:	Date: 05/11/22

Appendix 1

Definitions

Information security incident

Indicators of a potential or actual information security incident are:

- emails from unexpected or unidentifiable senders
- unexpected emails from people that you do know
- requests for information from unknown sources
- inability to access systems
- inability to access files or documents
- unusually slow systems or unexpected and strange behaviour of PCs and devices

Personal information

Personal information is recorded information or opinion about an identifiable individual. It can be almost any information linked to an individual, including name, address, sex, age, financial details, marital status, education or employment history. De-identified information about individuals can also be personal information if it has the potential to be re-identified.

Sensitive information

For the purpose of this policy and associated guidance material, sensitive information in schools includes but is not limited to the following:

- student information including name address and date of birth
- student academic records, progress reports, assignments and assessments
- student health and medication information
- student information pertaining to family circumstances including Intervention Orders and Family Court decisions
- student class photographs and individual images
- families' and carers' names, address, phone number, email address and custody instructions
- teachers personal information
- families' and carers' banking and credit card information and hard-copy records
- school financial information
- tendering and procurement documents
- vendor invoices, contacts and accounts payable and receivables

Summary of record keeping periods

Record name	Record keeping period	Legislation
Child enrolment records	Kept until the end of 3 years after the last date on which a child is educated and cared for by the service	Education and Care Services National Regulations - regulation 183(2)(d)
Documentation of child assessments	Kept until the end of 3 years after the last date on which a child is educated and cared for by the service	National Regulations – regulation 183(2)(d)
Evaluations for delivery of the educational program	Kept until the end of 3 years after the last date on which a child is educated and cared for by the service	National Regulations – regulation 183(2)(d)
Medication record	Kept until the end of 3 years after the last date on which a child is educated and cared for by the service	National Regulations – regulation 183(2)(d)
A record of attendance for each child for whom care is provided (regardless of eligibility for Child Care Subsidy), including records of any absences from care	Must be kept for seven years .	Family Assistance Law – section 219F(1)
A record relating to an incident, illness, injury or trauma suffered by a child	Must be kept in a safe and secure place until the child is 25 years of age	National Regulations – regulation 183(2)(b)
A record relating to the death of a child while being cared for by the service or may have occurred as a result of an incident	Must be kept in a safe and secure place until seven years after the death	National Regulations – regulation 183(2)(c)
All records relating to the nominated supervisor or a staff member at the service	Must be kept for three years from the last day they provided education and care on behalf of the service	National Regulations – regulation 183(2)(f)
Record of assessments of OSHC venues and spaces	Must be kept for three years after the record was made	National Regulations – regulation 183(2)(g)
Record of service's compliance with the National Law	Must be kept for three years after the record was made	Education and Care regulation
Complaints made to the provider, or to any of the services of the provider, relating to compliance with Family Assistance Law	Must be kept for seven years .	Family Assistance Law
Statements or documents demonstrating that	Must be kept for seven years .	Family Assistance Law

additional absence days in excess of the initial 42 absence days satisfy requirements (see Reporting absences).		
Copies of invoices and receipts issued for the payment of child care fees	Must be kept for seven years.	Family Assistance Law
Copies of all Statements of Entitlement issued and any statements issued to advise that there was a change of entitlement.	Must be kept for seven years.	Family Assistance Law
Any notice given to a state or territory body about a child at risk of abuse or neglect (to be documented)	Must be kept for seven years.	Family Assistance Law
Copies of the evidence and information provided with an application for approval about persons with management or control of a provider and persons responsible for the day-to-day operation of a service	Must be kept for seven years.	Family Assistance Law
Any evidence or information produced to obtain police checks and working with children checks for personnel and to support any statements about these checks in an application for provider or service approval.	Must be kept for seven years.	Family Assistance Law
Providers must keep written records of all required background checks for specified personnel	Must be kept for seven years.	Family Assistance Law

Appendix 3

Information security and data integrity

OSHC services and schools must protect the confidentiality, integrity and availability of school information. They will manage and share information appropriately and securely in order to meet information security obligations and to appropriately protect staff, students and their families.

Information security aims to protect the confidentiality, integrity and availability of school information. This includes the consideration of privacy compliance when dealing with personal information.

School councils and Principals must establish appropriate practices to protect critical and sensitive information. All staff should consider:

- what information they have
- how sensitive the information is
- where it is stored
- who has access to it

School councils and Principals are to make sure that information security risks and issues are appropriately managed by seeking advice from the Department of Education and Training InfoSafe team. The Pomonal Primary OSHC Person with Management Control or Nominated Supervisor will ensure that a third party software package used is approved for administering Child Care Subsidy.

Behaviours — Being InfoSafe

The consequences of an information security breach can be far reaching, potentially affecting staff, students and families. Pomonal Primary OSHC will make sure that the protection of information is embedded in all aspects of school operations as outlined in this policy. The Pomonal Primary OSHC Nominated Supervisor will:

- Ensure that priority actions from this policy are considered in appropriate local school practices and IT Committees
- Encourage staff to complete the [Information Security for School Staff eLearning module](#) (login required) on an annual basis
- Establish and maintain an InfoSafe culture through ongoing conversations with all levels of staff at OSHC.

Risks — Understanding information risks

Pomonal Primary OSHC will adopt a risk-based approach to information security by periodically assessing themselves against a school set of common, published risks and associated treatment plans. This will enable service and school treatment plans to be prioritised and actioned based on the extent of the risk. The Nominated Supervisor will:

- Refer to the [Pre-populated InfoSafe School Risk Document](#) and document OSHC and InfoSafe risks to be incorporated to the school's risk register
- Consider the IT environment, online tools and the nature of the information at Pomonal Primary OSHC.
- Consider the most common information security and privacy risks and their relevance at Pomonal Primary OSHC.

Access — Identify the appropriate access for the information at OSHC

Pomonal Primary OSHC must make sure that access to information is authorised for individuals based upon their role and function within the school environment. Failure to assign the right level of access to information to the right role may result in an information security or privacy breach. The Pomonal Primary OSHC Nominated Supervisor will:

- Identify who has access to sensitive information and who has privileged accounts at you're the OSHC service and school.
- Establish a process to capture and regularly review OSHC staff, and third-party access, including families and carers, volunteers and contractors
- Establish a process to enforce need-to-know access to sensitive information (revoke access in a timely manner)

Networks — Securing ICT networks

Schools must maintain a secure ICT network by following Departmental requirements and adopting appropriate technical controls. Without these controls the school information and systems will be vulnerable to cyber-attacks. The Pomonal Primary OSHC service will work collaboratively with the school's IT technician to:

- Regularly review network configuration and anti-virus and patching arrangements
- Confirm that any hardware or software used in the delivery of the OSHC service is compliant with Pomonal Primary's requirements by consulting appropriate staff at the school

Storage — Identifying and storing information appropriately

The OSHC service must identify their critical and sensitive information and store it in approved and trusted locations. The Nominated Supervisor will:

- Identify and document assets holding sensitive and critical information
- For systems holding personal information, ensure that the security processes [have been completed](#).
- Review school processes to identify where data is held long-term

Physical — Physical protection

The OSHC service must protect information and ICT equipment by housing all ICT infrastructure (servers and network equipment) and personal computers, when not in use, in a locked and secured location with restricted access. The Nominated Supervisor will:

- Monitor visitor entry to the service premises and authorise entry into infrastructure and records storage locations
- Ensure the OSHC service follows the school's local visitors policy and the Department's [Visitors in Schools Policy](#)
- Make sure that sensitive information (digital and hard copy) and ICT equipment is housed in physically secured locations. Refer also to [Records Management — School Records](#).

Awareness — Training and awareness

The OSHC service is responsible to encourage staff to be vigilant and aware of the ongoing need to protect sensitive school and OSHC information and systems. The Nominated Supervisor will:

- Encourage staff to complete the [Information Security for School Staff e-learning module](#) (login required) and complete this module annually.
- Act on Department information and directions about emerging cyber security threats
- Ensure the induction process for new staff, including contractors and casuals, includes the Information Security for School Staff eLearning module
- Regularly communicate, affirm and review security obligations for staff (and target specific roles that have access to sensitive information).

Sharing — Sharing information safely

Pomonal Primary OSHC must follow Department of Education and Training policies for sharing personal or sensitive information with other schools or anyone external to the school. The Nominated Supervisor will:

- Identify which personal and sensitive information is regularly shared or likely to be shared (typically personal data of staff or students, but potentially other categories of information e.g., financial, commercial). Refer to [Requests for Information about Students](#) and [Privacy and Information Sharing](#)

- Make sure staff are aware of Department policies and local procedures for sharing information. Refer to [Privacy and Information Sharing](#) and [Requests for Information about Students](#)
- Use only approved tools to transmit sensitive data and will closely manage distribution lists.

Suppliers — Externally sourced systems security

Pomonal Primary OSHC, schools and the Department must ensure the security of new systems and the suppliers who provide them. The Nominated Supervisor will:

- Seek advice from the InfoSafe team to ensure all new systems meet Information Security and ICT security requirements
- For those systems holding personal information, conduct a Privacy Impact Assessment (PIA) which includes a security assessment for that system.
- Support staff to access external resources are also available through Australian Cyber Security Centre and keep up to date by subscribing to the [Scamwatch](#) newsletter.

Records destruction

Pomonal Primary OSHC must not dispose of:

- any records that are reasonably likely to be required in a legal proceeding
- any record that may be required for a current Freedom of Information request

Pomonal Primary OSHC may dispose of temporary records that have reached the required retention period (the minimum period the records must be kept for before they can be legally destroyed). The principal must approve the disposal in writing to provide evidence of the disposal activity.

Pomonal Primary OSHC must securely dispose of records and ensure electronic and hardcopy records are destroyed in a way that ensures the records are unreadable and irretrievable. Pomonal Primary OSHC will adhere to the Department recommendation to use secure disposal bins for the disposal of hardcopy records.