

ATTACHMENT 1

RECORD KEEPING, RETENTION PERIODS AND STORAGE

The table below sets out the requirement for retaining different types of records and information in relation to children, the management of the kindergarten services, staff, volunteers and financial information. The files should be labelled with the destroy dates and those that contain confidential information should be password protected or securely stored.

Where there are data protection, including confidentiality issues containing personal information, paper records must be disposed of securely at the end of their retention period via security shredding or confidential waste bins.

Keeping Records and Retention Periods

Children's Records	Retention Period	Authority	Where Stored
Enrolment record	3 years after the child's last attendance at the service. Regulations 160, 177(1)(l), 178(1)(e) & 183	Australian Children's Education and Care Quality Authority (ACECQA)	Central Records with selected access: Xpedite enrolment system QikKids KIMS S:\General Central Enrolments Service Hard copy stored in a locked filing cabinet in an office. Past record achieved at the service in a secure location.
Attendance record	Until the end of 3 years after the last date on which the child was educated and cared for by the service. Regulations 158, 159, 177(1)(k), 178(1)(d) & 183	ACECQA	Central Records with selected access: Service Hard copy stored in a locked filing cabinet in office. When children are in attendance, record is on display for parents and staff to access. Past record archived at the service in a secure location.
Child's assessments or evaluations for delivery of the educational program	Until the end of 3 years after the child's last	ACECQA	Central Records with selected access:

	attendance at kindergarten. Regulations 74, 177(1)(a), 178(1)(a) & 183		Service Hard copy documents stored in a locked filing cabinet in office. Some hardcopy i.e. child's portfolio, available to children, staff and families to access while they are in attendance at the service. Soft copies online saved to service computer. Soft copies in online platforms e.g., Storypark. Past record archived at the service in a secure location.
Medication record	Until the end of 3 years after the child's last attendance at kindergarten. Regulations 92, 177(1)(c) & 178(1)(c) & 183	ACECQA	Central Records with selected access: Service Hard copy stored in a locked filing cabinet in office. Past record archived at the service in a secure location.
Incident, injury, trauma and illness	Keep the record until the child is 25 years old. Regulation 87, 177(1)(b), 178(1)(b) & 183,	ACECQA	Central Records with selected access: S:\OHS\OHS Policies & Procedures\OHS Register Service Hard copy stored in a locked filing cabinet in office. Past record archived at the service in a secure location.
Death of a child whilst being educated and cared for by the service	Keep the record until the end of 7 years after the child's death.	ACECQA	Central Records with selected access:

	Regulations 12 & 183(2)(c)		S:\OHS\OHS Policies & Procedures\OHS Register
Complaint record	3 years after the date on which the record was made	National Quality Framework (pg. 475)	Central Records with selected access: S:\General HR\HR Manager\Disciplinary or S:\General HR\HR Manager\Grievances
Personnel Records	Retention Period	Authority	Where Stored
Personnel files and training records for staff	7 years after employment ceases	Fair Work Regulations 2009	Central Records with selected access: S:\General HR\Scanned Staff Records Hard copy of current staff stored in a locked filing cabinet in office.
Records for volunteers	Until the end of 3 years after the volunteer attended the service. Regulation 149 & 183(2)(f)	ACECQA	Central Records with selected access: S:\General HR\Preschools\Student and Volunteer Hard copy of volunteers stored in a locked filing cabinet in office. Past record archived at the service in a secure location.
Records for students	Until the end of 3 years after the student attended the service. Regulations 149 & 183(2)(f)	ACECQA	Central Records with selected access: S:\General HR\Preschools\Student and Volunteer Hard copy of current students stored in a locked filing cabinet in office.
Records for Responsible Persons in day-to-day	Until the end of 3 years after the staff	ACECQA	Central Records with selected access.

charge including Nominated Supervisors placed in day-to-day charge	member works for the service Section 162 Regulation 145, 150 & 177		Hard copies at respective services: Hard copy stored in a locked filing cabinet in office. Past record archived at the service in a secure location.
Records for Educators working directly with children on the day	Until the end of 3 years after the staff member works for the service. Regulation 151 & 183(2)(f)	ACECQA	Central Records with selected access: S:\General HR\Scanned Staff Records and copies located at each respective service by staff member. Hard copy of current educators stored in a locked filing cabinet in office.
Application forms and interview notes for unsuccessful candidates	3 to 6 months following interviews	Australian Privacy Principles	Central Records with selected access: Destroyed if permission is not granted. Or S:\General HR\Scanned Staff Records\Pending new staff
Pay Records	Retention Period	Authority	Where Stored
Wages/salary records (including overtime, bonuses and expenses)	7 years	Fair Work Regulations 2009	Central Records with selected access: ADP Payforce S:\General Finance\Payroll
Redundancy details including calculations of payments	7 years from the date of redundancy	Fair Work Regulations 2009	Central Records with selected access: ADP Payforce S:\General Finance\Payroll
Parental leave record	7 years	Fair Work Regulations 2009	Central Records with selected access: ADP Payforce

			S:\General Finance\Payroll
Financial Records	Retention Period	Authority	Where Stored
Accounting and financial records, reports, workings and methodologies	7 years	Financial Management Act 1994	Central Records with selected access: S:\General Finance\End of Financial Year MYOB Advanced
Health and Safety Records	Retention Period	Authority	Where Stored
Staff accident record	3 years from the date of the last entry	OH&S Act 2012	Central Records with selected access: S:\OHS\OHS Policies & Procedures\OHS Register
Records of any reportable death, injury, disease or dangerous occurrence	3 years from the date of the last entry	OH&S Act 2012	Central Records with selected access: S:\OHS\OHS Policies & Procedures\OHS Register
OH&S Risk Assessments	Until the end of 3 years after the Approved Provider operated the service Regulation 183(2)(e) Until 3 years after the record was made Regulation 183(2)(g)	OH&S Act 2012 ACECQA	Central Records with selected access: S:\General HR\Preschools followed by respective kindergarten subfolder.
Excursion Risk Assessments	Until 3 years after the record was made. Regulations 100, 101 & 183(2)(g)	ACECQA	Central Records with selected access: S:\General HR\Preschools followed by respective kindergarten subfolder. Soft copy stored on the service computer.

			<p>Or</p> <p>Hard copy stored in a locked filing cabinet in office.</p> <p>Past record archived at the service in a secure location.</p>
WorkCover Employee Claim form	99 years	OH&S Act 2012	<p>Central Records with selected access:</p> <p>S:\OHS\OHS Policies & Procedures\OHS Register followed by respective staff's subfolder</p>
Administration Records	Retention Period	Authority	Where Stored
Insurance certificates	40 years from the date insurance commences or is renewed	DET	<p>Central Records with selected access:</p> <p>S:\General Finance\Insurance</p>
Meeting minutes	<p>Until 3 years after the record was made.</p> <p>Regulation 165 & 183(2)(g)</p>	ACECQA	<p>Central Records with selected access:</p> <p>Service meetings</p> <p>Soft copy stored on the service computer.</p> <p>May be shared using an online platform e.g., Microsoft Teams.</p> <p>Hard copy stored in a locked filing cabinet in office.</p> <p>Past record hard copy archived at the service in a secure location.</p> <p>Central office meetings</p> <p>S:\(location depending upon subject matter)</p>
Sign In/Visitor book	Until 3 years after the record was made.	ACECQA	Central Records with selected access:

	Regulation 165 & 183(2)(g)		<p>Hard copy stored in a locked filing cabinet in office.</p> <p>Past record archived at the service in a secure location.</p>
External correspondence (in and out) and internal memoranda	7 years	Shine Bright requirement	<p>Central Records with selected access:</p> <p>Soft copy using email or online platform e.g. Teams, on the service computer or via text message on service mobile.</p>
Internal reports, reviews, investigations, files, projects, workings and methodologies	7 years	Shine Bright requirement	<p>Central Records with selected access:</p> <p>Service documents</p> <p>Soft copy stored on the service computer.</p> <p>May be shared using an online platform e.g., Microsoft Teams.</p> <p>Hard copy stored in a locked filing cabinet in office.</p> <p>Past hard copies archived at the service in a secure location.</p> <p>Central office documents</p> <p>S:\(depending upon subject matter)</p>

Storage of Records

Shine Bright will ensure that sensitive and confidential information and all corporate records will be stored in a safe and secure location for the relevant time periods as identified in the '*Keeping Records and Retention Period*' table. These records will only be made accessible to relevant and authorised individuals.

Note: Information of this nature is attractive and valuable. Staff are to ensure they store this information correctly and with the requisite level of security required.

Shine Bright will ensure that information kept in a record is not divulged or communicated through direct or indirect means to another person other than:

- To the extent necessary for the education and care or medical treatments of the child to whom the information relates to,
- To a parent of the child to whom the information relates to, except in the case of information kept in a staff record,
- To the Regulatory Authority or an Authorised Officer,
- As expressly authorised, permitted or required to be given by or under any Act or Law,
- With the written consent of the person who provided the information, or
- As otherwise directed by the Chief Executive Officer and/or the Board.

If a kindergarten is transferred under the law, documents relating to a child must not be transferred without the express consent of the child's parent/s. It is the responsibility of the Transferring Provider to obtain this consent from families.

Records that relate to children and are to be kept 3 years or less, are to be kept at the relevant kindergarten.

Records that relate to children and that are to be kept for more than 3 years, will need to be scanned by staff at the service and saved electronically within appropriate security controls. Appropriate security controls involves saving the files on the most secure drive on the computer (currently the C drive) and to ensure that relevant usernames and passwords are used to access these files. Scanning documents is recommended to be part of Pack Up or Set Up days. Hard copy files are to be destroyed using security shredding options.

Storage and Protection of data

All data recorded electronically must be stored in approved locations as per Attachment 2: Electronic Records Approved Storage. This is to ensure Shine Bright has approved and adopted a consistent approach to protect data records from damage, misuse or loss.

Non-Approved Data Storage Devices

Staff are not permitted to input or store any information including photos relating to Shine Bright on a non-approved device (including desk top, lap top, smart phone, tablet or similar devices or removable storage devices and similar).

Storage locations not approved by Shine Bright may not be backed up by our IT provider and Shine Bright cannot guarantee that information stored on these systems can be retrieved if required. There is also no guarantee that adequate protection of information is in place in non-approved devices...

If Shine Bright information is temporarily or mistakenly or otherwise collected and stored on a non-approved device, all Shine Bright related information must be removed from the non-approved device

and immediately transferred to Shine Bright Central Records to ensure all relevant information is accessible by staff to use in their work.

Approved Data Storage Devices

Approved devices are those issued by Shine Bright or those privately owned but formally approved in writing for use by staff in conjunction with working for Shine Bright.

Only software added or approved by Shine Bright may be loaded onto an approved device. All data and records created on an approved device must be saved into Shine Bright Central Records for data storage so that required information can be easily accessible by authorised staff members.

Approved devices will be subject to periodic audit to ensure no unauthorised software has been loaded and used. Such Audits will occur without prior notice to monitor compliance with this policy, and to ensure that -

- No unapproved software is uploaded onto Shine Bright's computers or electronic devices,
- Only appropriate and approved malware is installed on computers and electronic devices,
- No illegal substances/media are contained on computers and electronic devices, and
- Storage of personal and corporate information complies with this Policy.