PRIVACY AND CONFIDENTIALITY POLICY

Privacy is acknowledged as a fundamental human right. Highland Grove Preschool has an ethical and legal responsibility to protect the privacy and confidentiality of children, individuals and families as outlined in Early Childhood Code of Ethics, Education and Care Services National Regulations and the Privacy Act 1988 (Cth). The right to privacy of all children, their families, and educators and staff of the Service will be upheld and respected, whilst ensuring that all children have access to high quality early years care and education. All staff members will maintain confidentiality of personal and sensitive information to foster positive trusting relationships with families.

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1	Governance	Governance supports the operation of a quality service
7.1.1	Service philosophy and purposes	A statement of philosophy guides all aspects of the service's operations.
7.1.2	Management Systems	Systems are in place to manage risk and enable the effective management and operation of a quality service.
7.1.3	Roles and Responsibilities	Roles and responsibilities are clearly defined and understood and support effective decision-making and operation of the service.
7.2	Leadership	Effective leadership builds and promotes a positive organisational culture and professional learning community.

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS	
168	Education and care services must have policies and procedures
181	Confidentiality of records kept by approved provider
181-184	Confidentiality and storage of records

PURPOSE

To ensure that the confidentiality of information and files relating to the children, families, staff, and visitors using the Service is upheld at all times. We aim to protect the privacy and confidentiality of all information and records about individual children, families, educators, staff and management by ensuring continuous review and improvement on our current systems, storage, and methods of disposal of records. We strive to ensure that all records and

information are held in a secure place and are only retrieved by or released to people who have a legal right to access this information. Our centre takes data integrity very seriously. We strive to assure all records and data is protected from unauthorised access and that it is available to authorised persons when needed. This policy provides procedures to ensure data is stored, used and accessed in accordance with relevant policies and procedures.

SCOPE

This policy applies to children, families, educators, staff, management, students, volunteers and visitors of the Service.

IMPLEMENTATION

Under National Law, Section 263, Early Childhood Services are required to comply with Australian privacy law which includes the *Privacy Act 1988* (the Act) aimed at protecting the privacy of individuals. Schedule 1 of the *Privacy Act* (1988) includes 13 Australian Privacy Principles (APPs) which all services are required to apply. The APPs set out the standards, rights and legal obligations in relation to collecting, handling, holding and accessing personal information.

The Notifiable Data Breaches (NDB) scheme requires Early Childhood Services, Family Day Care Services, and Out of School Hours Care Services to provide notice to the Office of the Australian Information Commissioner (formerly known as the Privacy Commissioner) and affected individuals of any data breaches that are 'likely' to result in 'serious harm'. Businesses that suspect an eligible data breach may have occurred, must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. A breach of an Australian Privacy Principle is viewed as an '*interference with the privacy of an individual*' and can lead to regulatory action and penalties.
(Source: OAIC Australian Privacy Principles)

Further information about the APPs is included in Appendix 1 of this policy.

The Approved Provider will:

- Ensure that obligations under the Education and care Service National law and national Regulations are met.
- ensure the Service acts in accordance with the requirements of the Australian Privacy Principles and *Privacy Act 1988* by developing, reviewing, and implementing procedures and practices that identify:
    - the name and contact details of the Service
    - what information the Service collects and the source of information

    - why the information is collected
    - who will have access to information
    - collection, storage, use, disclosure, and disposal of personal information collected by the Service
    - any law that requires the particular information to be collected
    - adequate and appropriate storage for personal information collected by the Service
    - protection of personal information from unauthorised access.
- ensure educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure and provided with a copy if required
- advise students, volunteers and visitors of their role to maintain confidentiality during induction
- ensure families are aware of the *Privacy and Confidentiality Policy*
- provide staff and educators with relevant information regarding changes to Australian privacy law and Service policy
- ensure all relevant staff understand the requirements under Australia's privacy law and Notifiable Data Breaches (NDB) scheme
- maintain currency with the Australian Privacy Principles (this may include delegating a staff member to oversee all privacy-related activities to ensure compliance).
- ensure personal information is protected in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012* and only authorised personnel have access to private and sensitive information
- ensure all records and documents are maintained and stored in accordance with Education and Care Service National Regulations
- regularly back-up personal and sensitive data from computers to protect personal information collected
- ensure all computers are password protected and install security software- antivirus protection
- ensure families are notified of the time particular records are required to be retained as per Education and Care Services National Regulations [regulation 183 (2)]
- ensure the appropriate and permitted use of images of children
- ensure the appropriate and permitted use of images of children, including obtaining written authorisation from parents and/or guardians of children who will be photographed by the Service. The authorisation is to state the purpose for which the images and videos are to be used for and details regarding their publication or sharing.
- ensure personal electronic devices including phones, smartwatches or other devices that are able to take images or videos, are not used in the children's environment
- ensure only devices that are issued by the Service are used to record and store images and videos of children

- develop procedures to ensure controls are in place over the storage, access and retention of children's images and videos at the Service, including hardcopy and digital files
- ensure all employees, students, volunteers, and families have access to a copy of this policy
- deal with privacy complaints promptly and in a consistent manner, following the Service's *Dealing with Complaints Policy* and procedures
- ensure families only have access to the files and records of their own children
- upon request from a parent, provide documents or information relating to their child
- refer to individual family court orders for guidance regarding access, sharing and release of information where required
- ensure information given to educators will be treated with respect and in a professional and confidential manner
- ensure individual child and staff files are stored in a locked and secure cabinet
- ensure information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions
- ensure that information shared with the Service by the family will be treated as confidential unless told otherwise

The Centre Director, Supervisor and/or Responsible Person will:

- ensure that obligations under the *Education and Care Services National Law and National Regulations* are met
- ensure the Service acts in accordance with the requirements of the Australian Privacy Principles and *Privacy Act 1988* by developing, reviewing, and implementing procedures and practices that identify:
    - the name and contact details of the Service
    - what information the Service collects and the source of information
    - why the information is collected
    - who will have access to information
    - collection, storage, use, disclosure, and disposal of personal information collected by the Service
    - any law that requires the particular information to be collected
    - adequate and appropriate storage for personal information collected by the Service
    - protection of personal information from unauthorised access.
- ensure educators, staff, students, and volunteers have knowledge of and adhere to this policy and associated procedure and provided with a copy if required
- advise students, volunteers and visitors of their role to maintain confidentiality during induction
- ensure families are aware of the *Privacy and Confidentiality Policy*

- ensure all relevant staff understand the requirements under Australia's privacy law and Notifiable Data Breaches (NDB) scheme
- ensure personal information is protected in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012* and only authorised personnel have access to private and sensitive information
- ensure all records and documents are maintained and stored in accordance with Education and Care Service National Regulations (See *Record Keeping and Retention Policy*)
- regularly back-up personal and sensitive data from computers to protect personal information collected
- ensure all computers are password protected and have security software-antivirus protection installed
- ensure families are notified of the time particular records are required to be retained as per Education and Care Services National Regulations [regulation 183 (2)]
- ensure the appropriate and permitted use of images of children, including obtaining written authorisation from parents and/or guardians of children who will be photographed by the Service. The authorisation is to state the purpose for which the images and videos are to be used for and details regarding their publication or sharing.
- ensure personal electronic devices including phones, smartwatches or other devices that are able to take images or videos, are not used for this purpose in the children's environment
- ensure only devices that are issued by the Service are used to record and store images and videos of children
- develop procedures to ensure controls are in place over the storage, access and retention of children's images and videos at the Service, including hardcopy and digital files
- deal with privacy complaints promptly and in a consistent manner, following the Service's *Dealing with Complaints Policy* and procedures
- ensure families only have access to the files and records of their own children
- refer to individual family court orders for guidance regarding access, sharing and release of information where required
- upon request from a parent, provide documents or information relating to their child
- ensure information given to educators will be treated with respect and in a professional and confidential manner
- ensure only necessary information regarding the children's day-to-day health and wellbeing is given to non-primary contact educators. For example, food allergy information.
- ensure individual child and staff files are stored in a locked and secure area.
- ensure information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions
- ensure that information shared with the Service by the family will be treated as confidential unless told otherwise

- ensure personal and sensitive information regarding the health and wellbeing of a child, family member or staff member is not shared with others unless consent has been provided, in writing, or provided the disclosure is required or authorised by law under relevant state/territory legislation (Reg. 177(4A))
- complete a *Privacy Audit* every 12 months or following a breach of data to ensure the Service meets lawful obligations, identifies areas for improvement and to detect potential areas of breach in privacy law
- follow the *Data Breach Response Procedure* and complete a *Data Breach Response Template* following any breaches in data at the Service
- ensure employees who have resigned acknowledge their commitment to refrain from accessing accounts or misusing sensitive and confidential information
- adhere to Service's policies and procedures at all times
- ensure educators, staff, volunteers, and families are aware of the *Privacy and Confidentiality Policy*
- ensure the Service obtains written consent from parents and/or guardian of children who will be photographed by the Service
- ensure families only have access to the files and records of their own children
- ensure that information given to Educators will be treated with respect and in a confidential and professional manner
- not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand
- ensure that information shared with us by the family will be treated as confidential unless told otherwise
- ensure information regarding the health and wellbeing of a child or staff member is not shared with others unless consent has been provided, in writing, or provided the disclosure is required or authorised by law under relevant state/territory legislation.

Educators, students and staff will:

- read and adhere to the *Privacy and Confidentiality Policy* at all times
- ensure documented information and photographs of children are kept secure but may be accessed at any time by the child's parents or guardian
- treat private and confidential information with respect in a professional manner
- ensure documented information and photographs of children are kept secure but may be accessed at any time by the child's parents or guardian
- ensure service documentation and records remain at the Service
- inform management if they learn of images of enrolled children being shared on social media or by any other format by families or staff that have been obtained via the Services'

app, Facebook page or other format; or photos taken during special events by the Service or families

- not use personal electronic devices in the environment with children. Phones, are to be kept in locked storage for staff
- ensure parents or guardians only have access to the files and records of their own children (unless a court order prohibits access)
- not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand
- ensure that information shared with the service by the family will be treated as confidential unless told otherwise
- maintain individual and Service information and store documentation according to this policy at all times
- ensure personnel and sensitive information is not accessed by unauthorised persons
- not disclose or share information about an individual or Service, management, or other staff (unless authorised to do so by legislation)
- ensure passwords used to gain access to private and sensitive information are not shared with others
- ensure any media enquiries are directed to the approved provider or nominated supervisor.
- not discuss individual childr
- en with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand.
- ensure that information shared with the service by the family will be treated as confidential unless told otherwise
- maintain individual and Service information and store documentation according to this policy at all times
- not share information about the individual or service, management information, or other staff as per legislative authority.

FAMILIES WILL:

- be aware of the *Privacy and Confidentiality Policy* upon enrolment
- ensure all information provided to the Service is accurate and kept up to date
- be informed that access to documentation and personal information is limited to their own child/ren
- follow the *Dealing with Complaints Policy* regarding any complaints or concerns regarding privacy and confidentiality of private and sensitive information

- share information relating to individual family court orders or parenting plans with the Service and update these as required
- ensure they do not share data or personal information of other family members, children or staff members from the Service with anyone, including other families of the same Service
- not use or share images obtained from the Service, via the Services app, Facebook pages or other format
- not share photographs taken during special events, that contain children other than their own, for publishing on any social media or for sharing in any format
- respect that staff are prohibited to share information about other children, families or staff members without expressed written consent to whom the information relates to.

Australian Privacy Principles- Personal Information

Highland Grove preschool (ABN:31207822712) is committed to protecting personal information in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012*.

Personal information includes a broad range of information, or an opinion, that could identify an individual.
Sensitive information is personal information that includes information or an opinion about a range of personal information that has a higher level of privacy protection than other personal information.
(Source: OAIC-Australian Privacy Laws, Privacy Act 1988)

Personal information will be collected and held securely and confidentially about you and your child to assist our Service provide quality education and care to your child whilst promoting and maintaining a child safe environment for all stakeholders.

Method of Collection

Information is collected using standard forms at the time of enrolment or employment
Additional information may be provided to the Service through email, surveys, telephone calls or other written communication.
Information may be collected online through the use of software such as CCS software or program software

How we protect your personal information

To protect your personal and sensitive information, we maintain physical, technical and administrative safeguards.

All hard copies of information are stored in children's individual files or staff individual files in a locked cupboard.
All computers used to store personal information are password protected. Each staff member will be provided with a unique username and password for access to CCS software and program software. Staff will be advised not to share usernames and passwords.
Access to personal and sensitive information is restricted to key personal only.
Data is regularly backed up on external drive and/or through a cloud storage solution
Any notifiable breach to data is reported
All staff are aware of the importance of confidentiality and maintaining the privacy and security of all information.
Procedures are in place to ensure information is communicated to intended recipients only, example invoices and payment enquiries

Access to personal and sensitive information

Personal and sensitive information about staff, families and children will be stored securely at all times.

The Approved Provider will ensure that information kept in a child's record is not divulged or communicated through direct or indirect means to another person other than:

- the extent necessary for the education and care or medical treatment of the child to whom the information relates
- a parent of the child to whom the information relates, except in the case of information kept in a staff record
- 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.

Disclosing personal and sensitive information

Our Service will only disclose personal or sensitive information to:

- a third-party provider with parent permission (for example CCS software provider)
- Child Protection Agency- Office of the Children's Guardian and Regulatory Authority as per our *Child Protection and Child Safe Environment Policies*
- as part of the purchase of our business asset with parental permission
- authorised officers (for example public health officer)
- the regulatory authority or an authorised officer
- as expressly authorised, permitted or required to be given by or required to be given by or under any Act or Law
- with the written consent of the person who provided the information.

Complaints and Grievances

If a parent, employee or volunteer has a complaint or concern about our Service, or they believe there has been a data breach of the Australian Privacy Principles, they are requested to contact the Approved Provider so reasonable steps to investigate the complaint can be made and a response provided.

If there are further concerns about how the matter has been handled, please contact the Office of Australian Information Commissioner on 1300 363 992 or:
https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC
For any other general concerns, please contact the Approved Provider directly on: 43676935.

APPENDIX

The Australian Privacy Principals (APPs) outline:

- The open and transparent management of personal information, including having a privacy policy
- An individual having the option of transacting anonymously or using a pseudonym where practicable
- The collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- How personal information can be used and disclosed (including overseas)
- Maintaining the quality of personal information
- Keeping personal information secure
- Right for individuals to access and correct their personal information

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'.

Sensitive information is a type of personal information and includes information about an individual's:

- Health (including predictive genetic information)
- Racial or ethnic origin
- Political opinions
- Membership of a political association, professional or trade association or trade union
- Religious beliefs or affiliations
- Philosophical beliefs
- Sexual orientation or practices
- Criminal record

Australian Privacy Principles (APPs)

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and Pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-order disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information
Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.
Source: Australian Government Office of the Australian Information Commissioner (OAIC)
https://www.oaic.gov.au/privacy/

Source

Australian Childcare Alliance. (2019). Changes to Australia's privacy law: What ECEC services need to know: https://childcarealliance.org.au/blog/115-changes-to-australia-s-privacy-law-what-ecec-services-need-to-know
Australian Children's Education & Care Quality Authority. (2014)
Australian Government Department of Education, Skills and Employment. *Child Care Provider Handbook (2018)*
https://www.dese.gov.au/resources-child-care-providers/resources/child-care-provider-handbook
Australian Government Office of the Australian Information Commission – Australian Privacy Principles: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
Early Childhood Australia Code of Ethics. (2016).
Education and Care Services National Law Act 2010. (Amended 2018).
Education and Care Services National Regulations. (2011).
Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. (2017).
Guide to the National Quality Framework. (2017). (Amended 2020).
Privacy Act 1988.
Revised National Quality Standard. (2018).
UN General Assembly (1989) United Nations Convention of the Rights of a child

REVIEWED: Currently under review- March 2024