CommunityOSH Privacy Statement

Our service recognises that every individual has the right to ensure their personal information is accurate and secure, and only used or disclosed to achieve the outcomes for which it was initially collected. Personal information will be managed openly and transparently in a way that protects an individual's privacy and respects their rights under Australian privacy laws.

Implementation

Our Privacy Notice and Disclosure Statement are at the end of this Policy.

Our Service practices are consistent with the Australian Privacy Principles.

Collection of personal information

We collect personal information if it is necessary for us to carry out Service operations or to comply with our legal obligations. This includes information required to comply with the National Education and Care Law and Regulations and to promote learning under the Early Years Learning Framework. Information may also be collected to comply with other Laws including State or Territory Health Laws.

During the enrolment process the Approved Provider will:

- explain what personal information we need to collect, why we need to collect it, whether the information is required or authorised by Law and how it may be shared.

Personal information includes name, address, date of birth, gender, family contact details, emergency contact details, authorised nominee details, parents' occupations, cultural background, home language, religious beliefs, payment details, child care benefit information, immunisation records, medical information, medical management plans, photos of children and family members and information about children's strengths, interests, preferences and needs, including special needs. Personal information also includes "government related identifiers" like Medicare numbers and CCB references.

- advise families about our Privacy and Confidentiality Policy and how to access it.
- attach a copy of our Privacy Notice to our Enrolment Form and other forms we use to collect personal information.
- verbally advise children's emergency contacts and authorised nominees that we have some of their personal information on file and explain the advice in the Privacy Notice.
- explain the advice in the Privacy Notice to individuals who provide personal information verbally (eg by phone).

We usually collect personal information directly from a parent or guardian either in writing or verbally, for example during enrolment, when completing waiting list applications, or as we establish a partnership with families in caring for and educating a child. We may also collect information through our website, social media page, Family Law court orders or agreements, special needs agencies and training courses.

We may occasionally request information from other organisations which you would reasonably agree is necessary for us to educate and care for a child. For example, we may request a copy of a child's immunisation records where they are transferring to us from another Service, or where we request information about a child from a special needs educator or organisation. We will not request information without obtaining the consent of the individual (or parent) concerned.

In most cases, if we are unable to collect relevant personal information, we will be unable to enrol a child at the Service.

The Approved Provider will advise individuals about any unsolicited personal information we receive from other organisations and keep because it is directly related to our functions and activities (unless we are advised not to by a Government authority). The Approved Provider will destroy any unsolicited personal information that is not directly related to our Service operations unless it adversely impacts the health, safety and wellbeing of a child or children at the service. If this happens the Approved Provider will contact the appropriate Government authorities and take action as directed while protecting the confidentiality of the individuals concerned.

Use or disclosure of personal information

We will not use personal information for any purpose that is not reasonably needed for the proper or effective operation of the service. Personal information may be accessed by and exchanged with staff educating and caring for a child or by administrative staff.

We do not disclose your personal information to others unless you would have reasonably expected us to do this or we have your consent. For example, personal information may be disclosed to:

- emergency service personnel so they can provide medical treatment in an emergency
- special needs educators or inclusion support agencies
- volunteers, trainees and work experience students (with consent)
- trainers or presenters if children participate in special learning activities
- another Service to which a child is transferring where you have consented to the transfer.
- the new operator of the Service if we sell our business and you have consented to the transfer of enrolment and other documents listed in Regulation 177 of the National Education and Care Regulations.

We may disclose personal information where we are permitted or obliged to do so by an Australian law. For example, personal information may be disclosed to:

- authorised officers when our service is assessed and rated under the National Education and Care Law and Regulations
- Government employees (eg for CCB, Immunisation, Medicare purposes)
- software companies that provide child care management systems
- management companies we may engage to administer the Service
- software companies that provide tailored computer based educational tools for children
- lawyers in relation to a legal claim.
- officers carrying out an external dispute resolution process
- a debt collection company we use to recover outstanding fees
- authorities if we are taking action in relation to unlawful activity, serious misconduct, or to reduce or prevent a serious threat to life, health or safety.

We do not disclose personal information to any person or organisation overseas or for any direct marketing purposes.

Quality of personal information

The Approved Provider will take reasonable steps to ensure the personal information we collect, use and disclose is accurate, current and complete. Educators and staff will:

- view original sources of information if practical when information is collected.
- collect and record personal information in a consistent format, for example using templates for enrolment, incident, injury, trauma and illness and administration of medication.
- record the date personal information was collected or updated.
- update information in our physical or electronic records as soon as it's provided.

In addition, the Approved Provider will:

- regularly remind families via emails or website to update their personal information including emergency contact details and their child's health information.
- ask parents to update their enrolment details annually, or whenever their circumstances change.
- verify the information is accurate, current and complete before disclosing it to any external organisation or person.
- ensure documentation about children and families is based on facts and free from prejudice.

Security of personal information

The Approved Provider will take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure. These steps include:

- taking responsibility for the security of personal information and regularly checking the practices implemented to protect it. This will include management of access privileges to ensure only people who genuinely need to see personal information can access it.
- ensuring information technology systems have appropriate security measures including password protection, anti-virus and 'malware' software, and data backup systems.

- ensuring physical repositories of personal information are secure with the Directors in a in a filing cabinet which is locked.
- ensuring all educators and staff are aware of their obligations in relation to the collection, use and disclosure of personal information, through activities like mentoring, staff meetings or on-line training courses.
- requiring all educators, staff, volunteers and work experience students to sign a 'Confidentiality Statement' acknowledging that personal information:
    - can only be accessed if it is necessary for them to complete their job
    - cannot be disclosed to other organisations (including colleges, RTOs) or discussed with individuals outside the service including personal family members unless they have written consent from the person (or parent) concerned.
    - must be stored in compliance with service practices which safeguard its security.
- ensuring records which we don't need to keep, including unsuccessful job applications and records which fall outside the record keeping timeframes under the National Education and Care Law and Regulations (refer to our Record Keeping and Retention Policy) are destroyed in a secure way as soon as possible by, for example, shredding, incinerating or permanently deleting electronic records including archived or back-up copies. Where possible, the destruction of records containing personal information will be overseen by two employees.
- 'de-identifying' personal information so that people (e.g. our accountant) who require the information may access it without being able to identify individuals. We will do this by providing only relevant information and details where/if required by law.
- 'de-identifying' personal information which may come into the public domain. For example, removing identifying names or details from newsletters etc.
- ensuring staff comply with our Social Media Policy (for example by obtaining authorisation from a child's parents before posting any photos of their child on the Service social media page, and not posting personal information on any social media page which could identify children or families.)
- ensuring confidential conversations with parents or with staff are conducted in a quiet area away from other children, parents and staff.

Breaches of Personal Information

The Approved Provider or Nominated Supervisor will implement the Service's Data Breach Response Plan and notify individuals and the Australian Information Commissioner (the Commissioner) if personal information is lost (hard copies or electronic), accessed or intentionally/unintentionally disclosed without authorisation, and this is likely to cause one or more persons serious harm.

Data Breach Response Plan

Employees must notify the Approved Provider or Nominated Supervisor about a breach or suspected breach of personal data as soon as they suspect the breach or become aware a breach has occurred. The Approved Provider or Nominated Supervisor will:

- quickly assess the situation to decide whether or not there has been a breach. This assessment must be completed within 30 days but given the potential for serious harm to individuals, should be completed as soon as possible
- record the nature of any data breach, and the steps taken to immediately contain the breach where possible and ensure it does not happen again. If necessary they will contact external experts for advice and guidance, for example on cybercrime (hacking) and information technology security measures like access, authentication, encryption and audit logs
- notify the Commissioner and the individuals where there is a risk of serious harm after a data breach
- liaise with their insurer to determine whether the insurance policy covers data breaches and any steps they need to take
- evaluate the effectiveness of their response to the data breach and implement improvements to the Plan if required after all notifications, records and remedial action are taken.

Serious harm

The Approved Provider or Nominated Supervisor will decide whether serious harm of a physical, psychological, emotional, financial or reputational nature is likely once fully informed about the type and extent of the breach. They will consider the type and sensitivity of the information, the type of security protecting the information if any (eg encryption) and how likely it is the information will be used to cause harm to individuals. Examples of the kinds of information that may increase the risk of

serious harm include sensitive information like an individual's health records, documents commonly used for identity fraud eg Medicare card, birth certificates and financial information.

The Approved Provider or Nominated Supervisor will also consider how long the personal information has been accessible because serious harm is more likely the longer it has been since the data breach.

Where a data breach occurs, there may be not always be a risk of serious harm. This may be the situation, for example, if a trustworthy person or organisation who has received personal information in error confirms they have not copied, and have permanently deleted the information, or where expert advice states it's unlikely encrypted data can be accessed.

Where they are satisfied there is no risk of serious harm, the Approved Provider or Nominated Supervisor are not required to notify individuals or the Commissioner about the breach. They may choose to advise the individuals concerned about the breach and the action taken. The Approved Provider or Nominated Supervisor will however appropriate keep records about the breach.

Notifying the Commissioner

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will prepare a Statement for the Commissioner which includes the name and contact details of the Approved Provider or Nominated Supervisor, a description of the data breach (including date occurred and detected and who obtained information), the type of information involved (why it may cause serious harm), and the steps individuals at risk of serious harm should take in response to the breach (eg steps to request new Medicare card or credit card). The Approved Provider or Nominated Supervisor will get specialist advice about the recommended steps if required. They may use the Notifiable Data Breach Form available online from the Office of the Australian Information Commissioner to notify the Commissioner.

Notifying Individuals

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will notify individuals about the breach as soon as possible using the most appropriate communication methods for the individuals concerned e.g. a telephone call, SMS, physical mail, social media post, or in-person conversation. The information provided is the same as that required for the Commissioner. It might also explain steps the Service has taken to reduce the risk of harm to individuals. The Approved Provider or Nominated Supervisor may notify everyone whose personal information was part of the breach or only those individuals at risk of serious harm. If this is not possible or practical, they may publish a copy of the Statement, for example on their website or Facebook page, and take steps to ensure individuals at risk of serious harm see the publication.

Access to personal information

Individuals may request access to their (or their child's) personal information and may request the correction of any errors. These requests may be made to the Approved Provider by telephone on 03 9977 3000 or email ADMIN@COMMOSH.NET.AU.

Personal information will be provided as soon as possible, and no later than 30 days from a request. We will provide the information in the form requested, for example by email, phone, in person, hard copy or electronic record unless it is unreasonable or impractical to do this for example due to the volume or nature of the information.

The Approved Provider will always verify a person's identity before providing access to the information and ensure someone remains with the individual to ensure information is not changed or removed without our knowledge.

There is no charge for making a request to access the information. However, we may charge a reasonable cost for staff, postage and material expenses if the information is not readily available and retrieving the information takes a lot of time. We will advise you of the cost and get your agreement before we proceed.

There may be rare occasions when we are unable to provide access because we believe:

- giving access would be unlawful, the information relates to unlawful activity or serious misconduct, or it may prejudice the activities of a law enforcement body.

- there is a serious threat to life, health or safety.
- giving access would unreasonably affect the privacy of others.
- the request is frivolous or vexatious, for example to harass staff.
- the information relates to legal proceedings (eg unfair dismissal claim) between the Service and the individual.
- giving access would reveal sensitive information about a commercial decision.

We may, however, provide the information in an alternative way for example by:
- deleting any personal information which cannot be provided
- providing a summary of the information
- giving access to the information in an alternative format
- allowing the individual to inspect a hard copy of the information and letting them take notes.

We will advise you promptly in writing if we are unable to provide access to the information, or access in the format requested. The advice will include the reasons for the refusal to provide the information (unless it is unreasonable to do this) and information about how to access our grievance procedure.

Correction of personal information

Individuals have a right to request the correction of any errors in their personal information. These requests may be made to the Approved Provider by telephone on 03 9977 3000 or email ADMIN@COMMOSH.NET.AU.

The Approved Provider will take reasonable steps to correct personal information that is inaccurate, out of date, incomplete, irrelevant or misleading as soon as it is available. The Approved Provider will:

- take reasonable steps to ensure information supplied by an individual is correct.
- verify the identity of an individual requesting the correction of personal information.
- notify other organisations about the correction if this is relevant, reasonable or practical.
- advise the individual about the correction to their information if they are not aware.
- if immediately unable to correct an individual's personal information, explain what additional information or explanation is required and/or why we cannot immediately act on the information provided.
- if unable to correct the information, include reasons for this (for example we believe it's current) and inform the individual about our grievance procedure and their right to include a statement with the information saying they believe it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.
- correct the information, or include a statement if requested, as soon as possible.

We will not charge you for making a request to correct their personal information or for including a statement with your personal information.

Complaints

If you believe we have breached Privacy Laws or our Privacy Policy may lodge a complaint with the Approved Provider by telephone on 03 9977 3000 or email ADMIN@COMMOSH.NET.AU. The Approved Provider will follow the Service's grievance procedure to investigate the complaint. Individuals who are unhappy with the outcome of the investigation may raise their complaint with the Office Australian Information Commissioner www.oaic.gov.au GPO Box 5218 Sydney NSW 2001 or GPO Box 2999 Canberra ACT 2601, phone 1300 363 992 or email enquiries@oaic.gov.au