NextSense Privacy Policy

Policy Summary – Key Points

- NextSense ensures all personal and sensitive information held by NextSense is handled responsibly and the dignity of each individual is respected in accordance with the *Privacy Act 1998* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**). Where applicable, NextSense also complies with its obligations under State or Territory Health Privacy Legislation.
- NextSense is committed to identifying privacy risks and where a risk has been identified implement, strategies to mitigate or manage those risks.
- This Policy outlines the circumstances in which we collect personal information, how we use and disclose that information.
- This Policy will also outline how any queries or concerns relating to the collection, use, storage and treatment of personal or sensitive information, are handled.
- This Policy also describes the principles for responding to a breach of data held by NextSense, including managing a data breach, and notification of persons whose privacy may be affected by the breach.

NextSense Privacy Policy

Part 1 – Purpose

NextSense takes its obligations regarding the management of personal and sensitive information provided to or collected by NextSense seriously. As part of our business activities, we ensure that all personal information held by NextSense is handled responsibly and the dignity of each individual is respected in accordance with the *Privacy Act 1998* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**). With respect to health records, NextSense complies with applicable state and territory legislation that prescribes how health service providers should handle your personal information including, but not limited to, health records.

With respect to all health records held by NextSense, we adhere to the NSW Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002* (NSW), the privacy principles arising in the *Health Records Act 2001* (VIC) and the *Privacy and Data Protection Act 2014* (VIC), *Health Records (Privacy and Access) Act 1997* (ACT), the *Information Privacy Act 2009* (QLD) and any other Health Privacy Laws in applicable States and Territories (collectively, **Health Information Acts**).

This Policy is intended to clearly describe how NextSense handles your personal information, including its collection, use, disclosure and security, and including any personal information we collect through our website. Under the Privacy Act, the APPs do not apply to NextSense's handling of employee records if it is directly related to a current or former employment relationship between NextSense and the individual.

NextSense is committed to identifying privacy risks and where a risk has been identified implement, strategies to mitigate or manage those risks. This Policy also describes the principles for responding to a breach of data held by NextSense, including managing a data breach, and notification to persons whose privacy may be affected by the breach. NextSense takes data security seriously and acknowledges that effective management of data breaches would assist NextSense in avoiding or reducing potential harm to both the affected individuals and NextSense and mitigate risk of future breaches.

NextSense may review and update this Policy to reflect any legislative changes, advancements in technology and in consideration of any changes to business operations and practices. Nothing in this Policy is intended to replace, remove or minimise any obligations arising under the Law.

Part 2 – Scope

This Policy applies to all individuals employed or engaged by NextSense, Board Directors, clients, students, parents/carers and donors. Where applicable, it also applies to all volunteers, contractors, secondees, affiliates and third parties.

Part 3 – Policy

3.1. What kinds of personal information is collected?

Personal information is information or an opinion about an individual from which they can be reasonably identified. The type of information collected and held by NextSense includes but is not limited to, personal information including health information and other sensitive information, about:

- Students and parents and/or guardians before, during and after the course of a student's enrolment at any of our school, preschool or kindergarten;
- Clients, and where applicable, their parents and/or guardians;
- Job applicants, staff members, volunteers, contractors and affiliates; and
- Other people who come into contact with NextSense.

NextSense may collect and hold the following types of information:

Personal information: names, addresses and other contact details, dates of birth, next of kin details, photographic images, attendance records, driver's licence information; and financial information, for example banking and finance details for payment of fees.

Sensitive Information: racial or ethnic origin, religious beliefs or affiliations, philosophical beliefs, professional memberships, government identifiers (e.g. Tax File Numbers), Court Orders (including but not limited to information relating to proceedings in the Family Court, Care and protection jurisdiction and apprehended violence orders), criminal records, Medicare number, NDIS number, other identifying or relevant insurance details relevant to service being provided by NextSense.

Health information: medical records, disabilities, immunisation details, treatment plans and specialist reports including psychological reports and vaccination records.

3.2. How is personal information collected?

3.2.1. Personal information provided by clients, parents and students

NextSense collects personal information through a variety of methods including electronic, telecommunication modes, completion of forms, digital platforms (for example through our website or apps) and face-to-face interactions. Where possible, we will collect your personal information directly from you or your authorised representative/s.

Where it is not reasonable for us to collect this information directly from you, NextSense may seek to collect this information from a third party.

With respect to its school, pre-school and kindergarten, NextSense may request personal information about a student or parent and/or guardians for the purposes of managing student enrolment and/or participation in any school, pre-school or kindergarten activity. In some

circumstances, if the requested information is not provided, NextSense may not be able to enrol or continue the enrolment of a student or permit the student to participate in a particular activity.

3.2.2. Personal information provided by a third party

In some circumstances NextSense may be provided with personal information regarding an individual from a third party, for example, a report provided by an external medical professional or reference from another school.

Third parties from whom NextSense may collect your personal information include:

- Other health service providers, including but not limited to healthcare professionals, hospitals, clinics and other allied health facilities if they have referred a client or are involved in the care of one of NextSense's clients;
- Other education providers;
- Responsible persons such as carers and relatives;
- The My Health Record program operated by the Commonwealth Department of Health, if the client has chosen to participate;
- Statutory bodies (as relevant); and
- Health insurers, law enforcement or other government bodies.

NextSense will collect sensitive information about an individual if such collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual where the individual whom the investigation concerns:

- Is physically or legally incapable of giving consent to the collection; and/or
- Physically cannot communicate consent to the collection.

In some circumstances, NextSense may receive information from the Office of the eSafety Commissioner for the purpose of supporting the resolution of a cyber bullying material complaint. NextSense may use information, including personal information of an individual disclosed by the eSafety Commissioner pursuant to the *Online Safety Act 2021* (Cth) to assist in the resolution of matters related to NextSense and any of its service areas.

3.3. Exception in relation to employee records

Under the Privacy Act, the APPs do not apply to an employee's record held by an employer. As a result, this Policy does not apply to the treatment of an employee record, where the treatment is directly related to the current or former employment relationship between the employer and employee.

3.4. Use of personal information

3.4.1. Use of client information

In relation to information collected regarding clients, NextSense's primary purpose of collection is to enable NextSense to provide health services and support to people with

hearing and vision loss. This includes providing adequate services to clients and meeting the needs of our clients.

The purposes for which NextSense uses personal information of clients include:

- Looking after client's health needs and delivering health services;
- To coordinate and/or communicate and collaborate with other healthcare providers involved in a client's care;
- To coordinate and/or communicate and collaborate with a team of internal and external health care professionals and specialists for the purposes of achieving health care outcomes and best practice in sensory disability services delivery;
- To procure additional healthcare services on an individual's behalf (such as referrals to other providers or obtaining second opinions);
- To conduct activities related to quality assurance/ improvement processes, risk management, audits, client satisfaction surveys and staff education and training;
- To liaise with any private health funds, Medicare, Department of Health, NDIS Commission, and other relevant departments as necessary;
- To fulfil regulatory and public health requirements including liaising with regulatory or health authorities as required by law;
- To send reminders of appointments, or client follow up and care notifications to the details provided by the client;
- To handle complaints or respond to anticipated or existing legal actions;
- Day to day administration;
- Satisfying NextSense's legal obligations; and
- Keeping clients updated with respect to developments in the field and seeking donations or support and providing marketing for NextSense.

3.4.2. Use of student and parent information

In relation to information collected regarding students and parents, NextSense's primary purpose of collection is to enable NextSense to provide schooling for the student. This includes satisfying the needs of parents, the needs of the student and the needs of NextSense throughout the entirety of the student's enrolment.

The purposes for which NextSense uses personal information of students and parents include:

- Management of students' educational, social, general well-being and health needs;
- Day to day administration;
- Delivering educational services;
- Satisfying NextSense's legal obligations;
- Provide for the operational needs of extra-curricular activities such as excursions;
- Keeping parents informed about matters relating to their child's schooling through correspondence, newsletters and magazines; and
- Seeking donations and marketing for NextSense.

3.4.3. Use of job applicants, staff members, contractors and volunteers' personal

information

In relation to personal information of job applicants, former and current employees, contractors and secondees, NextSense's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor. NextSense also obtains personal information about volunteers who assist NextSense in its functions or conduct associated activities, particularly with respect to volunteer work relating to children or other vulnerable persons.

The purposes for which this personal information is used by NextSense include:

- Administering the individual's employment or contract, as applicable;
- Insurance;
- Seeking donations and marketing for NextSense; and
- Fulfilling NextSense's legal obligations, for example with regards to child protection legislation, and health regulations.

3.4.4. Use of personal information through video surveillance

NextSense may use video surveillance for security purposes and the footage will be used by NextSense, and by the providers of our security services for security purposes only. Surveillance videos are not used by NextSense for any other purpose and the footage is not publicly available.

Surveillance cameras are not located in any toilets or change room facilities.

3.4.5. Use of personal information for marketing and fundraising

NextSense considers marketing and seeking donations as essential for the future growth and development of its services. Clients, parents, staff, contractors, volunteers and other members of the wider NextSense community may from time to time receive marketing or fundraising materials or information. NextSense is entitled to utilise personal information for the purpose of distributing such marketing materials, which are directly related to the services we provide in accordance with the applicable laws including but not limited to the Privacy Act and the *Spam Act 2003* (Cth).

In each direct marketing communication with the individual, NextSense will draw the individual's attention, or prominently display a notice, that should they wish to not receive any further direct marketing communication, they may opt out.

With the individuals consent and in compliance with the Privacy Act and Australian Privacy Principles, NextSense may also use personal information for the purposes of publications and marketing activities such as newsletters, magazines, stories and articles published on digital platforms and in hard copy.

An individual may withdraw their consent and/or advise NextSense that they do not wish to receive any marketing from NextSense at any time by using the opt-out facilities provided or by contacting:

- Email: hello@nextsense.org.au
- Call: 1300 581 391
- Text (SMS): 0451 562 273

NextSense will take reasonable measures to cease the collection, use or disclosure, or the further collection, use or disclosure of personal information of an individual who has opted out or withdrawn their consent.

3.5. Disclosure of personal and sensitive information

3.5.1. NextSense will only collect, use or disclose personal information that is:

- Reasonably necessary or directly related to our core functions and activities (our primary purpose); or
- For a directly related secondary purpose where the individual has provided consent; or
- Where it would be reasonably expected by the individual that we would disclose the information; or
- Where otherwise permitted under the Privacy Act or any other applicable law.

3.5.2. NextSense may disclose personal information, including sensitive information held about an individual, to:

- Healthcare service providers or other relevant parties involved in an individual's care, including requesting services on behalf of an individual;
- Statutory bodies when requested to do so by you or as required by law;
- Government or other statutory organisation, if required and in order to comply with our legal obligations;
- Other educational service, and teachers and relevant staff at that educational service operated by NextSense;
- Another educational entity;
- Trusted and authorised organisations and/or business and/or contractors and/or individuals providing professional, administrative, legal, consulting and financial services to NextSense;
- Recipients of NextSense publications, where consent has been obtained for such disclosure;
- Any organisation or entity either independent or affiliated with NextSense that assists NextSense with fundraising and marketing activities. We will not use or disclose sensitive information for the purpose of direct marketing unless you have consented to the information being used for that purpose;
- Any individual and/or entity you consent or authorise release of information to; and
- Any person or entity to whom NextSense are required to disclose the information to as a matter of law.

3.5.3. Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless the individual, or their authorised representative agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

3.6. Sharing of personal information within NextSense

In circumstances where an individual accesses more than one service offered by NextSense, we may share personal information collected from one service with the other related service within the organisation to facilitate holistic care and support for the individual and for administration purposes. We would not share sensitive information of an individual within the organisation unless the sharing of the information was directly relevant to the provision of a service to the individual.

In circumstances where NextSense is provided with or collects personal and sensitive information which may trigger reporting obligations to a statutory body pursuant to legislation, information may be shared within NextSense with authorised individuals who require the information to discharge their duty or responsibility within the organisation.

3.7. Sending and storing information overseas

3.7.1. NextSense may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or for the purposes of providing professional services to NextSense.

3.7.2. NextSense will ensure that any overseas provider of services is as compliant with privacy obligations as NextSense is required to be. Such disclosures will only be made if:

- The overseas recipient of the information is subject to laws, binding schemes or contract which effectively upholds the principles for fair handling of the information that are substantially similar to the APPs;
- The individual consents to the transfer (in some cases this consent will be implied); and
- NextSense has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the APPs.

3.7.3. In relation to the overseas transfer of personal information, if it is impractical for NextSense to receive the individual's consent to that transfer, NextSense must have sufficient reasons to believe that the person would likely give consent if they were contacted.

3.8. Management and security of personal information

3.8.1. NextSense has in place steps to protect the personal information held from misuse, interference, loss, unauthorised access, modification or disclosure by use of various methods including but not limited to access rights to computerised records.

3.9. Right to access and correct your personal information

3.9.1. Clients, student, parents and legal guardians, donors, and employees have a right to access personal information held about themselves and to advise NextSense of any perceived inaccuracy.

3.9.2. An individual may request to make changes to their privacy consent form, which is stored in their file.

3.9.3. Ordinarily, NextSense will refer any requests for consent and notices in relation to the personal information of a client or student who is a minor or where the individual does not have legal capacity, to the student's and/or client's parent/carers and/or authorised representatives, as applicable.

3.9.4. If NextSense is satisfied that any part of the information we hold about an individual is inaccurate, incomplete, out of date, misleading or irrelevant, subject to the purpose for which NextSense held this information, NextSense will take reasonable steps to amend that information.

3.9.5. NextSense can withhold the access of an individual to his or her information (and that of their child) in accordance with the Privacy Act. Such occasions may include, but are not limited to, where the release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of NextSense's duty of care to that individual, or if the release of information with interfere with an investigation.

3.9.6. If NextSense refuses the request to access information in accordance with an exception under the Privacy Act, or applicable Health Privacy Acts, the individual will be notified in writing setting out:

- Grounds for refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds for refusal under APP 12;
- The complaint mechanisms available to the individual; and
- Any other matters relevant under the law.

3.9.7. Requests to access personal information will be handled within any prescribed time period in accordance with the applicable legislation.

3.10. Response to data breaches

3.10.1. A data breach involves unauthorised access, disclosure or loss of personal information and may occur for a variety of reasons including intentionally or unintentionally.

3.10.2. NextSense will take appropriate, prompt action where we have reasonable grounds to believe that a data breach has, or is suspected to have occurred, as required by the Privacy Act. In such circumstances, NextSense will act in accordance with the *NextSense Response Plan to a Data Breach.*

3.10.3. The Privacy Act requires NextSense to notify affected individuals and the Office of

the Australian Information Commissioner (OAIC) about eligible data breaches. This occurs when the following criteria is met:

- There is unauthorised access to, or disclosure of, personal information held by NextSense (including a NextSense school, pre-school or kindergarten and any NextSense service), or information is lost in circumstances where unauthorised access or disclosure is likely to occur;
- This is likely to result in serious harm to any of the individuals to whom the information relates; and
- NextSense has been unable to prevent the likely serious harm with remedial action.

3.10.4. Where an eligible data breach is suspected or believed to have occurred, NextSense must:

- Carry out a risk assessment;
- Prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred;
- Submit the statement to the OAIC; and
- Consistent with any legal obligations, contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

3.11. NextSense's Website

3.11.1. NextSense collects statistical information about visitors to our websites using web analytics, which use cookies to assist us in understanding how visitor's access and utilise our website and information about our services.

3.11.2. Generally, this information does not contain personally identifiable information such as your name or email address and therefore cannot be used to identify an individual. In some circumstances it may include a visitor's internet protocol (IP) address, which could be linked to an individual.

3.11.3. This consolidated information provides a more accurate picture of visitor journeys and use of our services and website. Information that can directly identify an online visitor is collected only when offered by the visitor voluntarily via our online forms.

3.11.4. Our website may contain links to other websites of interest. NextSense does not control these websites or any of their content and where an individual chooses to visit these websites, NextSense is not responsible for or liable for the protection and privacy of any information which you provide whilst visiting such websites, and such websites are not governed by this Privacy Policy.

3.12. Enquiries and complaints

3.12.1. If you would like further information about this Privacy Policy, the way the NextSense manages the personal information it holds or wish to make a complaint

about an alleged breach of this Policy or the Privacy Act by NextSense, you should contact the Privacy Officer in writing at privacy@nextsense.org.au.

3.12.2. NextSense will investigate any complaint and will notify the individual of a decision in relation to their complaint as quickly as possible and within thirty (30) days from the date of receipt of the compliant, unless there are extenuating circumstances that lead to a reasonable delay. NextSense will notify you if the matter cannot be finalised within thirty (30) days.

3.12.3. If you are not satisfied with our response, you may refer the complaint to the OAIC.

3.12.4. If your concern relates to the management of health records, you may make a complaint to the OAIC or, depending on the applicable State or Territory:

- The NSW Information and Privacy Commissioner
- The Health Complaints Commissioner, Victoria
- The ACT Health Services Commissioner
- The Queensland Health Ombudsman
- The Health and Community Services Complaints Commission

Part 4 – Definitions

Affiliate	A person employed by an external entity who is formally affiliated with NextSense to conduct work as required by NextSense (for example Children's Hospital employees).
Cyber-bullying material	Refers to material in the form of text, data, speech, music, sounds, visual images (moving or otherwise), or in other form, provided on an online service, that is likely to have the effect of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating an individual.
Document	Includes anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.
Employee Record	As defined by the *Privacy Act 1988* (Cth)
eSafety Commissioner	Is an independent regulator granted power under the *Online Safety Act 2021* (Cth) to support and promote

	online safety and provide a complaints service for the reporting of cyber-bullying or illegal online content.
Health Information	Is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service.
Notifiable data breach	Occurs when there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information held by NextSense, where the access or disclosure of this information is likely to result in serious harm to one or more individuals and where NextSense hasn't been able to prevent the risk of serious harm with remedial action.
Personal Information	Is defined by the Privacy Act as meaning information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It includes all personal information regardless of its source.
Primary purpose	Is the purpose for which the personal information was collected. The relevant Collection Notices state the primary purpose for collection of personal information is to enable NextSense to provide support and services to people with hearing and vision loss. NextSense can only use or disclose personal information for the primary purpose or for a secondary purpose, if an exception applies.
Privacy Officer	Director of People and Governance, Manager: Quality, Compliance and Legal or their delegate.

Record	Includes a document or an electronic or other device. The Privacy Act regulates personal information contained in a 'record'. Items which are excluded from the definition of record relevant to NextSense are generally available publications and anything kept in a library, art gallery or museum for the purpose of reference, study or exhibition.
Remedial action	Is any action taken by NextSense to remove or reduce access to the information, such as ensuring information shared accidentally is recovered or deleted.
Secondary purpose	Is explained under APP 6 and includes, but is not limited to occasions where the individual has consented to a secondary use or disclosure of the personal information, where such disclosure is required or (authorised under law including an order of a court or tribunal), the individual would reasonably expect NextSense to use or disclose the personal information for the secondary purpose and that purpose is related to the primary purpose or, a permitted general situation exists in relation to the secondary use or disclosure.
Sensitive Information	Includes information or opinion relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information about an individual; and health information about an individual.
Serious Harm	To an individual may include serious physical, psychological, emotional, financial or reputational harm. The seriousness of the harm is gauged by the number of individuals whose personal information is involved. What information may have been accessed and its sensitivity, by whom, and their potential intentions. The *Privacy Act 1988* (Cth) sets out a non-exhaustive list of 'relevant matters' to consider the likelihood of serious harm.

Unauthorised access	Involves revealing personal information by a staff member, contractor, student or a third party who would not normally be permitted access.
Unauthorised disclosure	Involves making personal information available beyond NextSense without any legitimate grounds for disclosure.

Part 5 – Related Documents

This policy document should be read in conjunction with:

Legislation:

- *Privacy Act 1998* (Cth)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Health Records Act 2001* (VIC)
- *Privacy and Data Protection Act 2014* (VIC)
- *Information Privacy Act 2009* (QLD)
- *Health Records (Privacy and Access) Act 1997* (ACT)
- Australian Privacy Principles

Policy and Procedures:

- NextSense Privacy Notice
- Event-specific consent for information, images and recordings and privacy notice
- NextSense Code of Conduct Policy (POL00009)
- Feedback Policy (POL00030)
- Information and Communication Resource Policy (POL00017)
- Client Record Management Policy (POL00004)
- Social Media Policy and Guidelines (POL00008)
- NextSense Data Breach Response Plan