The Armidale Waldorf School
and Boongaiai Preschool
FOR RUDOLF STEINER EDUCATION

Privacy Policy

This Privacy Policy sets out how The Armidale Waldorf School manages personal information provided to or collected by it.

The School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Amendment Act 2012. In relation to health records, the School is also bound by the New South Wales Health Privacy Principles, which are contained in the Health Records and Information Privacy Act 2002.

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

What kinds of personal information does the School collect and how does the School collect it?

The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

• students and parents/guardians before, during and after the course of a student's enrolment at the School

• job applicants, staff members, volunteers and contractors

• other people who come into contact with the School

• photographs and other digitally recorded images of students

a) Personal Information provided: The School will generally collect personal information held about an individual by way of forms filled out by parents/guardians or students, face-to-face meetings and interviews, emails and telephone calls. On occasions, people other than parents/guardians and students provide personal information.
b) Personal Information provided by other people: In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.
c) Exception in relation to employee records: Under the Commonwealth Privacy Amendment Act 2012 and Health Records and Information Privacy Act 2002 (NSW), the Australian Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee.

How does The Armidale Waldorf School use the personal information it receives?

The School will use personal information it collects for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

a) Students and Parents/guardians: In relation to personal information of students and parents/guardians, the School's primary purpose of collection is to enable the School to provide schooling for the student. This includes satisfying the needs of parents/guardians, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School.

The purposes for which the School uses personal information of students and parents/guardians include:

- to keep parents/guardians informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the School;
- looking after students' educational, social and medical wellbeing;
- seeking donations and marketing for the School; and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

b) In some cases where the School requests personal information about a student or parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity. This is to ensure the safety of all.

c) Job applicants, staff members and contractors: In relation to personal information of job applicants, staff members and contractors, the School's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be. The purposes for which the School uses personal information of job applicants, staff members and contractors include:

- in administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the School; and
- to satisfy the School's legal obligations, for example, in relation to child protection legislation.

d) Volunteers: The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as alumni associations, to enable the School and the volunteers to work together and the School to fulfill its legal obligations and to discharge its duty of care.

e) Marketing and fundraising: The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising, for example an alumni organisation or, on occasions, external fundraising organisations. Parents/guardians, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications such as

newsletters and magazines, which include personal information may be used for marketing purposes.

Who might the School disclose personal information to and store your information with?

The School may disclose personal information, including sensitive information, held about an individual to:

• another school

• government departments

• medical practitioners

• people providing services to the School, including specialist visiting teachers, counsellors and sports coaches

• recipients of School publications

• parents/guardians

• the school's student accident insurance provider

• anyone you authorise the School to disclose information to

• anyone to whom we are required to disclose the information to by law

Sending and storing information overseas.

The School may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

• obtaining the consent of the individual (in some cases this consent will be implied);or

• otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The school, as set out below in the procedures, will not permit IT contractors to store backup copies of school data on overseas servers.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual. Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of students' and parents/guardian's personal information and the privacy of individuals. The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

The School will also ensure that contractors and software suppliers that have access and/or store backup copies of data containing students, parents/guardians and staff personal information are made aware of the School's Privacy Policy and also the requirement to advise the school of any possible Data Breach as set out in the Procedures for Data Breach found below. The Data stored by external servers is also to be encrypted to minimise the risk of being hacked.

Access and correction of personal information

Under the Commonwealth Privacy Amendment Act 2012 and the Health Records and Information Privacy Act 2002, an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. Students are able to access and update their personal information through their parents/guardians.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information the School holds about you or your child, please contact the School in writing. The School may require you to verify your identity and specify what information you require.

The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

The School respects every parent/guardian's right to make decisions concerning their child's education. Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents/guardians. The School will treat consent given by Parents/guardians as consent given on behalf of the student, and notice to Parents/guardians will act as notice given to the student.

Parents/guardians can indicate on the Permission to Publish Form provided at enrolment if they wish to refuse permission for photographs or digital recordings of their child(ren) to be used in publicity material of all types including on social media.

Parents/guardians may seek special access to personal information held by the School about them or their child by contacting the Education Director. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their parents/guardians. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

Enquiries and complaints

The School has appointed two Privacy Officers, the Education Director and the Business Manager who are responsible for Privacy compliance within the school.

Further information about the way the School manages the personal information it holds can be provided by the Privacy Officers. Should a concern arise about a possible breach of the Australian Privacy Principles please contact the Privacy Officers. The School will investigate any complaint and will notify you of the outcome in relation to your complaint as soon as is practicable. The School also has a Complaints and Grievance Policy which is available via the office.

Procedures for Privacy Policy

1. A summary of the school's Privacy Policy is to be included in the Parent and Staff Handbook and include details of where to find the full Policy
2. All staff and student records are to be filed in secure file cabinets with a key and archived appropriately with access only by key
3. The school server which contains information on students and staff is to only be accessed with a password and which drivers on the school server are to be accessed is to be determined by the Business Manager
4. All records that contain personal/sensitive information, that need to be discarded are to be placed through the opening in the locked blue wheelie bin in the photocopy room, which is shredded by a shredding service. Records that contain personal/sensitive information are not to be thrown into the regular bin.

Procedures for Provision of IT Services

5. If the school is procuring new contractors to provide IT Services they must be provided with a copy of the School's Privacy Policy and be made aware of and follow the Procedures for Data Breach
6. If the contractor/provider is providing a data back up service the backup must not be stored overseas
7. Microsoft 365's Data is currently held on servers within Australia however this service would need to be reviewed if they announced they are changing to store the data overseas.

Procedures for Data Breach

The following procedures are to be followed in response to the actual or suspected access to or disclosure of loss of personal information (Data Breach). Further guidance about responding to a Data Breach and an eligible data breach (EDB) is available and should be referred to under the Notifiable data breaches scheme (NDB Scheme) from the *Office of the Australian Information Commissioner.*

Response Plan

In the event of a Data Breach, school staff must adhere to the four-phase process set out below (As described in the *Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches scheme: Resources for agencies and organisations)*. It is important that appropriate records and any evidence are kept of the Data Breach and the response.

Response Team

The Business Manager, Education Director, and a Board Director or other appointed staff.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The School staff member or IT Contractor who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify The Business Manager or Education Director. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. The Business Manager or Education Director must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally
Medium	Loss of some personal information records and the records do not contain sensitive information Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures
Low	A few names and school email addresses accidentally disclosed to trusted third parties (eg where email accidentally sent to wrong person) Near miss or potential event occurred. No identified loss, misuse or interference of personal information

4. Where a **High Risk** incident is identified, the Business Manager or the Education Director must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. The Business Manager and Education Director must escalate **High Risk** and **Medium Risk** Data Breaches to the response team
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Data Breach, including by:
    a. identifying the type of personal information involved in the Data Breach;
    b. identifying the date, time, duration, and location of the Data Breach;
    c. establishing who could have access to the personal information;
    d. establishing the number of individuals affected; and
    e. establishing who the affected, or possibly affected, individuals are.
3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an EDB.
4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB
5. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach notifications

1. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
2. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.
3. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.
4. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.
5. The Response team will also advise the school's insurer and follow the necessary process required from them.

Phase 4. Take action to prevent future Data Breaches

1. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
2. The Business Manager must enter details of the Data Breach and response taken into a Data Breach log (saved on the Management Drive of the Server). The Business Manager must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
3. The Business Manager must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.
4. The Business Manager must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
5. The Business Manager must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.