PRIVACY POLICY

PRIVACY POLICY V1 2018

The Privacy Policy sets out how Chrysalis Montessori School protects your privacy and how we comply with the requirements of the Privacy Act and the 13 National Privacy Principles. The policy also describes:

- Who we collect information from;
- The types of personal information collected and held by us;
- How this information is collected and held;
- The purposes for which your personal information is collected, held, used and disclosed;
- How you can gain access to your personal information and seek its correction;
- How you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry will be handled; and
- Whether we are likely to disclose your personal information to any overseas recipients.

WHO DO WE COLLECT PERSONAL INFORMATION FROM?

At Chrysalis Montessori School we collect personal information from students, parents/guardians/carers (The Parent), prospective parents, job applicants, staff members, Board members, volunteers and others including alumni, contractors, visitors and others that come into contact with the school.

It is noted that employee records are not covered by the Australian Privacy Principles where they relate to current or former employment relations between the school and the employee.

WHAT KINDS OF PERSONAL INFORMATION DO WE COLLECT?

The kinds of personal information we collect is largely dependent upon whose information we are collecting and why we are collecting it, however in general terms the school may collect:

- **Personal Information** including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images and attendance records.
- **Sensitive Information** (particularly in relation to student and parent records) including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional or union memberships, family court orders and criminal records.

 Health Information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

 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.

HOW DO WE COLLECT YOUR PERSONAL INFORMATION?

How we collect personal information will largely be dependent upon whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from you. Where possible the school has attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form or a Health Form).

However, given the nature of our operations, we often also receive personal information by email, letters, notes, over the telephone, in face to face meetings, through financial transactions. We may also collect personal information from other people (e.g. a personal reference) or independent sources (e.g. a telephone directory), however we will only do so where it is not reasonable and practical to collect the information from you directly.

Sometimes we may be provided with your personal information without having sought it through our normal means of collection. We refer to this as "unsolicited information". Where we collect unsolicited information we will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the information as appropriate.

HOW WE USE PERSONAL INFORMATION

We only use personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by you, or to which you have consented.
Our primary uses of personal information include but are not limited to:

Student and Parents:

 Providing education, pastoral care, extra-curricular and health services;

 Satisfying our legal obligations including our duty of care and child protection obligations;

 Keeping parents informed as to school community matters through correspondence, newsletters and magazines;

 Marketing, promotional and fundraising activities;

 Supporting community based causes and activities, charities and other causes in connection with the School's functions or activities;

 Helping us to improve our day to day operations including training our staff; systems development; developing new programs and services; undertaking planning, research and

statistical analysis;

- School administration including for insurance purposes, debt collection
- The employment of staff;
- The engagement of volunteers
- Supporting the activities of parent support groups
- Supporting the activities of the alumni

We only collect sensitive information reasonably necessary for one or more of these functions or activities, if we have the consent of the individuals to whom the sensitive information relates, or if the collection is necessary to lessen or prevent a serious threat to life, health or safety, or another permitted general situation (such as locating a missing person) or permitted health situation (such as the collection of health information to provide a health service) exists.

If we do not have the relevant consent and a permitted health situation or permitted general situation does not exist, then we may still collect sensitive information provided it relates solely to individuals who have regular contact with the school in connection with our activities. These individuals may include students, parents, volunteers, former students and other individuals with whom the school has regular contact in relation to our activities.

We will only use or disclose sensitive information for a secondary purpose if you would reasonably expect us to use or disclose the information and the secondary purpose is directly related to the primary purpose.

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 to engage the applicant, staff member or contractors, as the case may be. The purposes for which the school uses personal information of job applicants, staff members, and contractors included:

- 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 schools legal obligations for example in relation to child protection legislation.

Volunteer:

The school also obtains personal information about volunteers who assist the school in its function or conduct associated activities, to enable the school and the volunteers to work together.

Marketing, fundraising and events:

The school treats marketing and seeking donations for the future growth and development of the school as an important part of ensuring the School continues to provide an outstanding learning environment in which both students and staff thrive.

STORAGE AND SECURITY OF PERSONAL INFORMATION

We store personal information in a variety of formats including on databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices. The security of your personal information is of importance to us and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.

These steps include:

- Restricting access to information on the school's databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile as outlined in the Information Security Protocol Appendix A.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring that hard copies of sensitive health information are stored in lockable filing cabinets and archive room. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the school buildings and grounds to prevent break-ins.
- Implementing policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Personal information we hold that is no longer needed is destroyed in a secure manner, deleted as appropriate.

Our website may contain links to other websites. We do not share your personal information with those websites and we are not responsible for their privacy practices. Please check their privacy policies.

WHEN WE DISCLOSE PERSONAL INFORMATION

We only use personal information for the purposes for which it was given to us, or for purposes which are related (or directly related in the case of sensitive information) to one or more of our functions or activities. We may disclose your personal information to government agencies, other parents, other schools or colleges, medical practitioners, recipients of school's publications, visiting teachers, counsellors and coaches, our service providers, agents, contractors, business partners and other recipients from time to time, only if one or more of the following apply:

- You have consented;
- You would reasonably expect us to use or disclose your personal information in this way;
- We are authorised or required to do so by law;

 Disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety;

 Where another permitted general situation or permitted health situation exception applies;

 Disclosure is reasonably necessary for a law enforcement related activity.

PERSONAL INFORMATION OF STUDENTS

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information.

At Chrysalis Montessori School we take a common sense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. We will treat notices provided to parents/carers as notices provided to students and we will treat consents provided by parents/carers as consents provided by a student.

We are however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. We also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers.

There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the school's duty of care to the student.

DISCLOSURE OF PERSONAL INFORMATION TO OVERSEAS RECIPIENTS

We may disclose personal information about an individual to overseas recipients in certain circumstances, such as when we are organising an overseas excursion, facilitating a student exchange, or storing information with a "cloud computing service" which stores data outside of Australia. We will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

 We have the individual's consent (which may be implied); or

 We have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime; or

 We form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or

 We are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

HOW WE ENSURE THE QUALITY OF YOUR PERSONAL INFORMATION

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date. These steps include ensuring that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. On an ongoing basis we maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed.

Please contact us if any of the details you have provided change. You should also contact us if you believe that the information we have about you is not accurate, complete or up to date.

HOW TO GAIN ACCESS TO YOUR PERSONAL INFORMATION WE HOLD

You may request access to the personal information we hold about you, or request that we change the personal information, by contacting us.

If we do not agree to provide you with access, or to amend your personal information as requested, you will be notified accordingly. Where appropriate we will provide you with the reason/s for our decision.

If the rejection relates to a request to change your personal information you may make a statement about the requested change and we will attach this to your record.

NOTIFICATION OF DATA BREACH

If the school discloses your personal information without your permission and not in accordance with this policy, and such a breach is likely to result in serious harm the Principal will be informed. The Principal will notify you directly.
If there is unauthorized access to our information systems and this breach is likely to result in serious harm, we the Principal will be informed. The Principal will notify you and include a description of the breach, the kinds of information concerned and the steps to be taken because of this Data breach. (The Principal will also inform the Australian Information Commissioner (OAIC) if required depending on the breach.)

PRIVACY COMPLAINTS

If you wish to make a complaint about a breach by us of the Australian Privacy you may do so by providing your written complaint by email, letter, facsimile or by personal delivery to any one of our contact details as noted below. You may also make a complaint verbally.

We will respond to your complaint within a reasonable time (usually no longer than 10 business days) and we may seek further information from you in order to provide a full and complete response.
Your complaint may also be taken to the Office of the Australian Information Commissioner.

HOW TO CONTACT US

You can contact us about this Policy or about your personal information by:

- Emailing admin@chrysalis.wa.edu.au
- Calling +61 8 9444 6025
- Writing to our Bursar at 3-5 Parkland Road, Glendalough WA 6016

If practical, you can contact us anonymously (i.e. without identifying yourself). However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

CHANGES TO OUR PRIVACY AND INFORMATION HANDLING PRACTICES

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website http://www.chrysalis.wa.edu.au regularly for any changes.

Approved by Mark Panaia, Principal

Status	V1
Owner	Principal
Principal Author	Mark Panaia
Reviewed	April 2018
To be reviewed	July 2020

Appendix A

Information and Data Security Protocol

Classification of Information/Data

A. Restricted Information

Information should be classified as Restricted when the unauthorized disclosure, alteration or use of that data could cause a significant level of risk to individuals or the School. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements and the School Privacy Policy. The highest level of security controls will be applied to Restricted information. The use or disclosure of information or data in this classification cannot be used for personal gain or profit and can only be authorised by the Principal.

B. Private Information

Information should be classified as Private when the unauthorized disclosure, alteration or use of that data could result in a moderate level of risk to individuals or the School. By default, all school data that is not explicitly classified as Restricted or Public information should be treated as Private information. A reasonable level of security controls should be applied to Private Information. The use or disclosure of information or data in this classification cannot be used for personal gain or profit and can only be authorised by the Principal.

C. Public Information

Information should be classified as Public when the unauthorized disclosure, alteration or use of that data would result in little or no risk to individuals or the School. While little or no controls are required to protect the confidentiality of Public information, some level of control is required to prevent unauthorized modification or use of Public Information.

Security Levels

LEVEL 1 – Public information

LEVEL 2 – Disclosure and use of information would not cause material harm but which the school chooses to keep confidential.

LEVEL 3 – Disclosure and use of information could cause risk of material harm to individuals or the school.

LEVEL 4 – Disclosure and use of information would be likely to cause serious harm to individuals or the school.

LEVEL 5 – Disclosure and use of information would cause severe harm to individuals or the school.

School information Security Levels

Security Level	Information/Data	Security Clearance	Classification
LEVEL 1	Name	Public	Public
LEVEL 2	Phone number	Admin/Staff	Private
LEVEL 3	Address	Admin/Staff/Board	Private
LEVEL 4	Email Address	Parent Liaison Person/Teachers/Admin	Restricted
LEVEL 5	Medical/Psych Reports/Court Orders	Admin	Restricted