The Montessori School Kingsley Inc.

PRIVACY AND MEDIA POLICY

Version Management

Version	Date Published/Reviewed	Changes Made	Author of Changes	Ratified by School Council
1	**01/01/2004**			
2	**23/3/2018**	**Update Policy as per changes to Privacy Act**	**Principal**	**April 2018**

PRIVACY POLICY

Your privacy is important
This statement outlines the Montessori School's policy on how the School uses and manages personal information provided to or collected by it.

The School adheres to the Australian Privacy Principles contained in the Commonwealth Privacy Act.

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

What kind of personal information does the School collect and how does the School collect it?
The type of information that the School collects and holds includes (but is not limited to) personal information, including sensitive information about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School, including:
    - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
    - parents' education, occupation and language background;
    - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
    - conduct and complaint records, or other behaviour notes, and school reports;
    - information about referrals to government welfare agencies;
    - counselling reports;
    - health fund details and Medicare number;
    - any court orders;
    - volunteering information; and
    - photos and videos at School events;
- job applicants, staff members, volunteers and contractors, including:
    - name, contact details (including next of kin), date of birth, and religion;
    - information on job application;
    - professional development history;
    - salary and payment information, including superannuation details;
    - medical information (e.g. details of disability and/or allergies, and medical certificates);
    - complaint records and investigation reports;
    - leave details;
    - photos and videos at School events;
    - workplace surveillance information; if applicable
    - work emails and private emails (when using work email address) and Internet browsing history; and
- other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

Personal information you provide:
The School will generally collect personal information held about an individual by way of forms filled out by parents or students, face to face meetings and interviews, and telephone calls. On occasions people other than parents and students provide personal information.

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.

Exception in relation to employee records:
Under the Privacy Act the Australian Privacy Principles do not apply to an employee record. As a result, the 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 will the School use the personal information you provide?
The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Pupils and Parents:

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

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

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

Personal information may be accessed by teaching or administrative staff of the School. Where the School requests personal information about a student or parent, and the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student

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 funds and promotion of the School
- to satisfy the School's legal obligations, for example, in relation to child protection legislation
- Personal information may be accessed by administrative staff of the School

Volunteers:

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

Promotion and fundraising:

The School treats promotion and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to be a quality learning environment in which both students and staff thrive. Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for promotional purposes.

Who might the School disclose personal information to?

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

- the International Baccalaureate Organisation
- another school
- government departments
- medical practitioners
- people providing services to the School, including specialist visiting teachers and sports coaches
- recipients of School publications, like newsletters and magazine
- parents or guardians
- anyone you authorise the School to disclose information to
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the School;
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

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)
- otherwise complying with the Australian Privacy Principles
- ensuring the recipient adheres to the Australian Privacy Principles

The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

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
- Sexual preferences, criminal record, that is also personal information
- Health information about an individual
- Other personal information

Sensitive information about an individual 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.

All records are stored securely, and regularly audited. Back-up of digital records is regularly performed, with back-up records stored off campus. Destruction of records may only be authorised by the Principal or the School Council. Paper records will be shredded and electronic records erased permanently. Records stored on hard-drives are destroyed through comprehensive wiping of hard-drive.

Updating personal information
The School endeavours to ensure that the personal information it holds is accurate, complete and up to date. A person may seek to update their personal information held by the School by contacting the Secretary of the School at any time. The National Privacy Principles require the School not to store personal information longer than necessary.

You have the right to check what personal information the School holds about you
Under the Commonwealth Privacy Act, 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. There are some exceptions to this right set out in the Act. Students will generally have access to their personal information through their parents, but older students may seek access themselves.

To make a request to access any information the School holds about you or your child, please contact the Principal in writing.

The School may require you to verify your identity and specify what information you require.

Consent and rights of access to the personal information of pupils
The School respects every parent'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. The School will treat consent given by parents as consent given on behalf of the student, and notice to parents will act as notice to the student.

Parents may seek access to personal information held by the School about them or their child by contacting the Principal. 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. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warrant it.

Enquiries and Complaints
If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles please contact the school principal in writing. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

MEDIA POLICY

1. Occasionally, the School Council or the Principal may authorise the photographing or videotaping of students and the School for the promotion of the School or of Montessori education. Permission will be sought from parents prior to the use of such photographs.

2. Audio and video recordings of students required for assessment purposes in IB Diploma courses. These recordings are sent overseas, and copies are stored securely at the school. This material is securely destroyed 12 months after the end of the relevant examination session.

3. Photographs of students will, in general, not be published with the students' names. Specific permissions will be sought for any exceptions to this.

4. Authority will be given to the Montessori School staff, on request, to photograph in the School for School records and copies will be made available for parents to view.

5. Authority will be given to others to photograph, audiotape or videotape in the School only after permission has been sought and obtained. Requests for permission to photograph, audiotape or videotape in the School will be made in writing to parents and formal consent obtained.

6. Parents who do not wish their child to be photographed or videotaped at any time should register their objection with their child's teacher.

7. Parents must complete a Photograph Permission Form on enrolment and on an annual basis thereafter.

8. On enrolment to the IB Programme parents must complete a Photographic Permission Form for IB Students which will cover students for all the years they are in the IB Programme.

RECORDS MANAGEMENT

The School keeps record relating to its operations. These records are managed efficiently and effectively to enable the good functioning of the School.

Employment records:

As an employer, the School is in possession of records relating to its employees. Records are kept according to the requirements of the Awards and Acts under which persons are employed. They are kept securely, and may only be accessed by the employee, their employer and relevant administrative staff and authorised government inspectors or organisation officials. They include but are not limited to:

- General employee records
- Pay records
- Hours of work records
- Leave records
- Superannuation contribution records
- Appraisal and other related records

Employee records are retained for a period of seven years after the departure of the employee. Destruction of records may only be authorised by the Principal or School Council. Paper records will be shredded and electronic records erased permanently.

Student records:

The School is in possession of documents and records relating to students. They are kept securely, as directed by the School's Privacy Policy and the Australian Privacy Principles. They include, but are not limited to:

- Class rolls and attendance data
- Reports
- Correspondence relation to students
- Records relating to student health, such as immunisation or medication records
- Records relating to student behaviour
- Records relating to student welfare
- Records relating to student learning
- Records relating to student learning

Student records are retained until after the student has turned 25 years of age. Destruction of records may only be authorised by the Principal or the School Council. Paper records will be shredded and electronic records erased permanently.

Other records:

Other documents and records relating to the operation of the School are also managed by the School. They are kept securely as directed by the School's Privacy Policy and the Australian Privacy Principles. They include, but are not limited to:

- Council minutes
- Principal's diary and correspondence
- Annual report
- Minutes of staff meetings
- Review or registration reports and correspondence with relevant authorities, such as the DES, IBO or MAF
- Strategic plans
- Plans, drawings, tender information, certificates
- Budget and financial papers
- Legal opinions, directions and files
- Asset register
- Archive and document destruction registers
- WHS minutes and records
- Visitors' books
- Parent correspondence
- Correspondence, emails and notes between the school and parents and/or third parties about a student registered at school

Records are retained for the relevant required period. Destruction of records may only be authorised by the Principal or the School Council. Paper records will be shredded and electronic records erased permanently.

PRIVACY & MEDIA PROFORMAS

Privacy Collection Notice

Photographic Permission Form

Photographic Permission Form – IB Students

Annexure 1

Annexure 2

Annexure 3

The Montessori School
PRIVACY COLLECTION NOTICE

The Montessori School, Kingsley Inc. collects information of a personal and sensitive nature as part of the application and enrolment of your children at the school. The collection and storage of this information is governed by the Privacy Policy The Montessori School, Kingsley Inc, set down in accordance with the *Australian Privacy Principles contained in the Commonwealth Privacy Act* which regulates the way private sector organisations, including non-government schools, handle 'personal information of individuals. The information collected may be passed on to a third party if required, but in accordance with the requirements of the Act. The Privacy Policy of The Montessori School Kingsley Inc. is available on our website www.themontessorischool.wa.edu.au

1. The School collects personal information, including sensitive information about pupils and parents or guardians before and during the course of a pupil's enrolment at the School. The primary purpose of collecting this information is to enable the School to provide schooling for your son/daughter.
2. Personal information collected by the school will be handled in accordance with the School's Privacy Policy and the Privacy Act. On request, a copy of the Privacy Policy and/or Records Management Policy will be supplied.
3. Some of the information we collect is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.
4. Certain laws governing or relating to the operation of schools require that certain information is collected. These include Public Health and Child Protection laws.
5. Health information about pupils is sensitive information within the terms of the Australian Privacy Principles under the Privacy Act. We ask you to provide medical reports about pupils from time to time.
6. The School from time to time discloses personal and sensitive information to others for administrative and educational purposes. This includes to other schools, government departments, medical practitioners, and people providing services to the School, including specialist visiting teachers, sports coaches and volunteers.
7. If we do not obtain the information referred to above we may not be able to enrol or continue the enrolment of your son/daughter.
8. Personal information collected from pupils is regularly disclosed to their parents or guardians. On occasions information such as academic and sporting achievements, pupil activities and other news is published in School newsletters, magazines and on our website.
9. Parents may seek access to personal information collected about them and their son/daughter by contacting the School. Pupils may also seek access to personal information about them. However, there will be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the School's duty of care to the pupil, or where pupils have provided information in confidence.
10. As you may know the School from time to time engages in fundraising activities. Information received from you may be used to make an appeal to you. We will not disclose your personal information to third parties for their own marketing purposes without your consent.
11. We may include your contact details in a class list and School directory. If you do not agree to this you must advise us now.

12. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.

ANNUAL PHOTOGRAPH PERMISSION FORM

Dear Parents

At certain times throughout the year, our students may have the opportunity to be photographed or filmed for our school publications, such as the school's newsletter or website, or to promote the school in newspapers and other media.

The School is the 'official photographer' for all school events on school property. Parents and visitors must not photograph film or digitally record any student or events on school property.

Rather than sending out permission letters on each occasion that we use photographs, we are sending a general request for permission to use your child's photograph should the need arise. Special permission will be sought if we wish to use your child's image for any other purpose.

Permission will not be required if a student is included in a background or group scene and is not clearly identifiable.

We would like your permission to use your child's photograph/video for the above purposes. Please complete the permission form below and return to the school by _____.

Thanking you for your cooperation.

MaryAnne D'Souza
Principal
The Montessori School, Kingsley Inc.

PHOTOGRAPHIC PERMISSION FORM 20xx

Name of Child …….. Teacher.....

I give permission for my child's photograph/video and name to be published in:

- the school website
- promotional materials
- newspapers and other media.

Name of Parent/Guardian (please circle) _____

Signed: Parent/Guardian …… Date ……..

If student is aged 15+, student must also sign:

Signed: Student …….. Date ……..

PHOTOGRAPH PERMISSION FORM - IB STUDENTS

Dear Parents

At certain times throughout the year, our students may have the opportunity to be photographed or filmed for our school publications, such as the school's newsletter or website, or to promote the school in newspapers and other media.

The School is the 'official photographer' for all school events on school property. Parents and visitors must not photograph film or digitally record any student or events on school property.

Rather than sending out permission letters on each occasion that we use photographs, we are sending a general request for permission to use your child's photograph should the need arise. Special permission will be sought if we wish to use your child's image for any other purpose.

Permission will not be required if a student is included in a background or group scene and is not clearly identifiable.

We would like your permission to use your child's photograph/video for the above purposes. Please complete the permission form below and return to the school by _____.

Thanking you for your cooperation.

MaryAnne D'Souza
Principal
The Montessori School, Kingsley Inc,

PHOTOGRAPHIC PERMISSION FORM IB STUDENTS

Name of Child …….. Teacher……..

I give permission for my child's photograph/video and name to be published in:

- the school website
- promotional materials
- newspapers and other media.

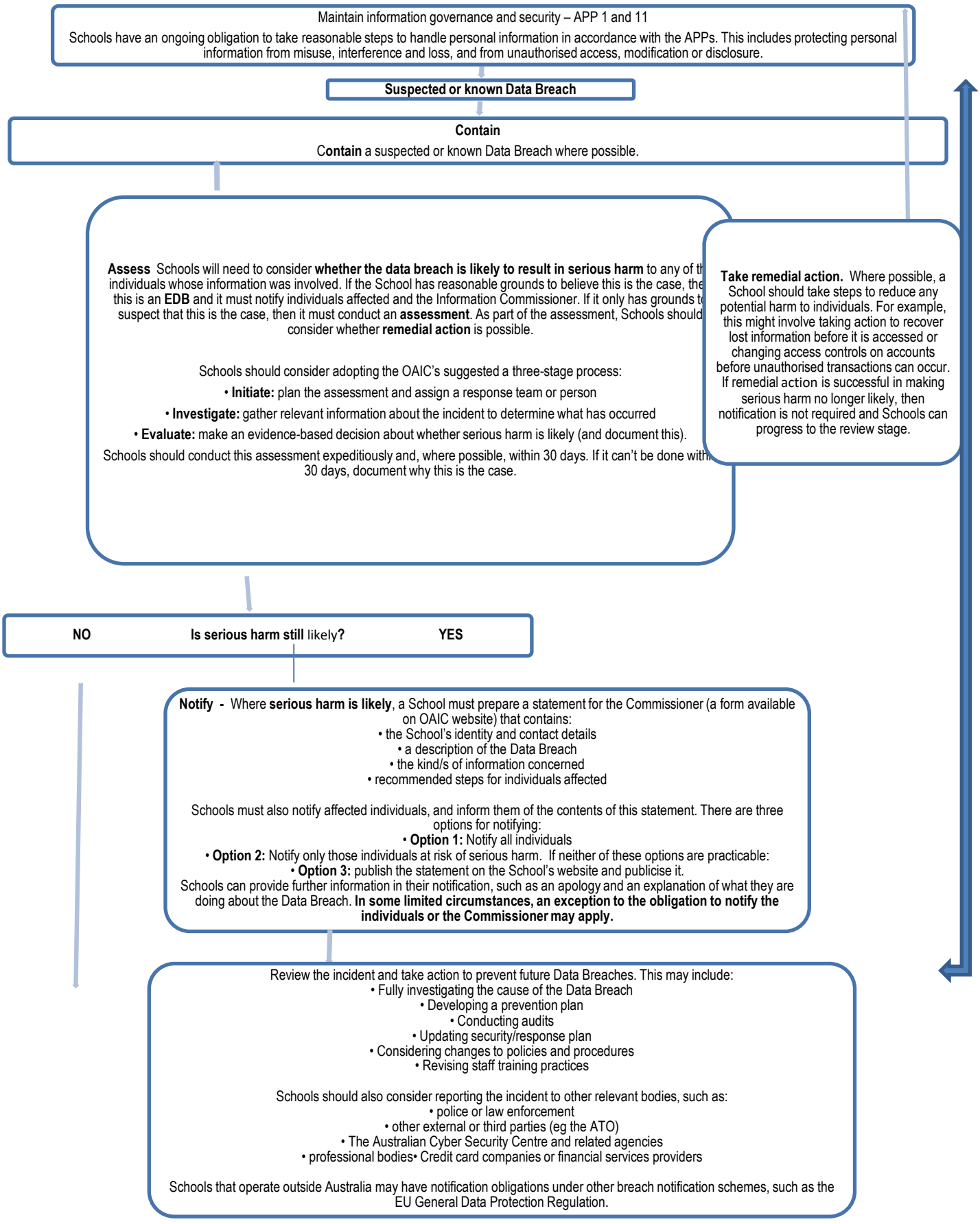
Name of Parent/Guardian (please circle) _____

Signed: Parent/Guardian …… Date ……..

If student is aged 15+, student must also sign:

Signed: Student …….. Date ……..

ANNEXURE 1 – MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES SUMMARY



This summary is a modified version of the OAIC Data Breach response summary available at www.oaic.gov.au/privacy-'aw/privacy-act/notifiable-data-breaches-scheme

ANNEXURE 2 – DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about	
Who is affected by the breach?	Are pupils, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a pupil's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Consider the kind or kinds of personal information involved	
Does the type of personal information create a greater risk of harm?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	For example, a disclosure of a list of the names of some pupils who attend the School may not give rise to significant risk. However, the same information about pupils who have attended the School counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of pupils or parents would also create more significant risks.
Who has gained unauthorised access to the affected information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a pupil's name, address and grades without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the pupil may be unlikely.
Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches is considered. This could involve incremental breaches of the same School database, or known breaches from multiple different sources (eg multiple schools or multiple data points within the one school).
How could the personal information be used?	Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual

	and social or workplace bullying)? For example, information on pupils' domestic circumstances may be used to bully or marginalise the pupil and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?
Is there evidence of intention to steal the personal information?	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.
What was the source of the breach?	For example, was it external or internal? Was it malicious or unintentional? Did it involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the School fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.
Is this a systemic problem or an isolated incident?	When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there

	may be more information affected than first thought, potentially heightening the risk.
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.

Assess the risk of harm to the affected individuals.	
Who is the information about?	Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/special needs, vulnerable families/parents)
What kind or kinds of information is involved?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) or a combination of personal information may pose a greater risk of harm to the affected individual(s) if compromised.
How sensitive is the information?	The sensitivity of the information may arise due to the kind of information involved, or it may arise due to the context of the information involved. For example, a list of the names of some pupils who attend the School may not be sensitive information. However, the same information about pupils who have attended the School counsellor or students with disabilities.
Is the information in a form that is intelligible to an ordinary person?	Examples of information that may not be intelligible to an ordinary person, depending on the circumstances may include: (i) encrypted electronic information; (ii) information that the School could likely use to identify an individual, but that other people likely could not (such as a pupil number that only the School uses – this should be contrasted to a pupil number that is used on public documents); and (iii) information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the School may need to consider the likelihood of the encryption algorithm being broken in the long term.
Is the information protected by one or more security measures?	For example, are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attack and stopped the attacker from accessing any information or copying the information?
If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?	For example, could an attacker have overcome network security measures protecting personal information stored on the network?

What persons (or kind of persons) have obtained or could obtain the information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a pupil's information without malicious intent, the risk of serious harm may be unlikely.
What is the nature of the harm that could result from the breach?	Examples include identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships, or workplace or social bullying or marginalisation. For example, information on pupils' domestic circumstances may be used to bully or marginalise the pupil and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.
Any other relevant matters?	The nature of other matters that may be relevant will vary depending on the circumstances of the School and the Data Breach.
Assess the risk of other harms.	
What other possible harms could result from the breach, including harms to the School or AISWA?	Examples include loss of public trust in the School or AISWA, damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

ANNEXURE 3 – DATA BREACH RESPONSE PLAN

Response plan

In the event of a Data Breach, School personnel 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. Legal advice should also be sought if necessary.

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

1. The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the Principal. The Principal will 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 Principal 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 party (e.g. 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 Principal must consider if any of the affected individuals should be notified immediately where serious harm is likely.

5. The Principal must escalate **High Risk** and **Medium Risk** Data Breaches to the response team (whose details are set out at the end of this protocol).

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 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

6. 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.

7. 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.

8. 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.

9. 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.

Phase 4. Take action to prevent future Data Breaches

10. 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.

11. The Principal must enter details of the Data Breach and response taken into a Data Breach log. The Principal must, every year, review the Data Breach log to identify any reoccurring Data Breaches.

12. The Principal 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.

13. The Principal must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.

13. The Principal 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.

Response Team

Position	Contact Email	Roles
Principal	principal@themontessorischool.wa.edu.au	See Phases 1,2,3,4
Office Manager	admin1@themontessorischool.wa.edu.au	See Phases 2,3,4
Reporting Staff Member		See Phases 1,2,3,4