Rockingham Montessori School Incorporated
ABN: 68 115 270 695

POLICY TITLE: Privacy Policy

BOARD APPROVAL DATE: July 2020 SIGNED BY CHAIR:

BOARD REVIEW DATE: July 2023

OVERVIEW:

Rockingham Montessori School Privacy Policy sets out how the School manages personal information provided to or collected by it.

Rockingham Montessori School is bound by the Australian Privacy Principles contained in the *Commonwealth Privacy Act 1998.* In relation to health records, the School is also bound by the National Privacy Principles contained in the Privacy Act 1988.
The school will review and update this Privacy Policy on a three year basis in order to take into account 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?

RATIONAL:

Rockingham Montessori School collects and holds personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School;
- job applicants, staff members, volunteers and contractors; and
- other people who come into 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 pupils, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than parents and pupils 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 and National Privacy Principles. The National 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.

GUIDELINES:

How will the School use the personal information you provide?

Rockingham Montessori 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 are reasonably expected and have been consented to. Personal information may also be used or released if it is believed that this is necessary for safety or legal reasons.

Pupils and Parents

In relation to personal information of pupils and parents, the School's primary purpose of collection is to enable the School to provide schooling for the pupil. This includes satisfying the needs of parents, the needs of the pupil and the needs of the School throughout the whole period the pupil is enrolled at the School. The purposes for which the School uses personal information of pupils and parents include:

- to keep parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the School;
- looking after pupils' 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.

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

Identity information is usually needed for the school to be able to fulfil its function as an educational institution or fulfil its duty of care obligations. On occasions where a person can deal with the school anonymously or by using a pseudonym, for example, when making a general inquiry about the school, the right to remain anonymous should be obliged as much as possible.

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.

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.

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 pupils and staff thrive. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising. Individuals may request not to receive direct marketing, either from the school or from the organisations directly. They may also request that the information not be used or disclosed to other entities for the purpose of facilitating direct marketing.

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 including images of people may be used for marketing purposes.

Who might the School disclose personal information to?

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

- another school in accordance with the *Schools Assistance (Learning together through Choice and Opportunity) Act*;
- government departments;
- medical practitioners;
- people providing services to the School, including specialist visiting teachers, counsellors and sports coaches;
- recipients of School publications, such as newsletters and magazines;
- parents or guardians;
- anyone the parent authorises the School to disclose information to; and
- anyone to whom the school is required to disclose the information to by law

Sending and storing information overseas:
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 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 and education applications. Information stored in the 'cloud' may be stored on servers outside Australia.
An example of such a cloud service provider is Microsoft, which provides platform services to the school including email and online education services (Teams). School personnel and service providers may have the ability to access, monitor, use or disclose emails, communications, documents and associated data for the purposes of administration and ensuring proper use.

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 only be collected by the school with your consent, unless required by law, under specific circumstances covered by law or if it is unreasonable or impracticable to obtain consent and collection of sensitive information is necessary to prevent or lessen a serious threat to the life or health of any 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 pupils' and parents' personal information and the privacy of individuals. Staff are trained on the school's information handling policies and practices.
Personal information is stored via secure means. 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. Where information is required to be present in a classroom or outside of school grounds, care is taken to prevent unauthorised access. These processes are reviewed on an ongoing basis to confirm they are complying with the relevant privacy legislation and access to electronic data such as firewalls are continually monitored. Privacy is considered in the design and implementation of any new data systems.
In the event that information is released to a contractor in order for them to perform their duties, stipulations are placed in the contract in order to protect the personal information disclosed and the contractor is monitored to ensure compliance. Contracting agencies, including providers of online services, should have a stipulation in their contract that the contractor must notify the school if there is a data breach affecting personal information and provide assistance to the school in responding to any data breach.
Records are audited for accuracy prior to use and records or information no longer needed is de-identified or destroyed via secure means (see also Record Management Policy). Families are offered the opportunity to update their information on a regular basis.

Access and correction of personal information

Under the Commonwealth Privacy Act [and the Health Records 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. Pupils will generally be able to access and update their personal information through their parents, but older pupils may seek access and correction themselves. 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 Principal 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 and, if possible, provide alternative options to satisfy the reason for the request. The School will respond to the request within a reason period, usually 30 days. If the School decides not to correct personal information in response to a request, a statement will be associated with that information to reflect that the individual has sought its correction and the reason for it e.g. inaccurate, out of date, incomplete, irrelevant, misleading.

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 pupil to the pupil's parents. The School will treat consent given by parents as consent given on behalf of the pupil, and notice to parents will act as notice given to the pupil. As mentioned above, parents may seek access to personal information held by the School about them or their child by contacting the School Principal. Access may be denied if the release would unreasonably impact upon duty of care, privacy or impact the School legally.

The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil 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 pupil and/or the pupil's personal circumstances so warranted.

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 the School has breached the Australian Privacy Principles please contact the School Principal. The School will acknowledge receipt of the complaint and endeavour to provide a response complaint as soon as is practicable after it has been made. If a more detailed investigation is required, the complaint may take longer to resolve, however, the school will endeavour to keep you informed of the complaint's status. This will be done in writing, if required by law.

The School reserves the right to verify the complainant's identity and seek appropriate information from the complainant and other relevant individuals in connection to the complaint. If complainant refuses to provide this information, the school has the right to refuse to proceed with the investigation. Similarly, the school reserves the right to refuse to investigate or deal with a complaint that the School considers to vexatious or frivolous.

If the complainant is dissatisfied with the outcome of the complaint, an internal review of the school's decision may be sought. If the complainant remains dissatisfied the complaint may be escalated the Office of the Australian Information Commissioner.

Privacy Breach

A privacy breach occurs when there is a loss, unauthorised access to or unauthorised disclosure of personal information. Examples of privacy breaches include loss of school equipment containing personal information, cyberattacks resulting in potential or actual access or loss of personal information, accidental transmission of personal information to unintended recipients via email, and misuse of personal information of students or parents by school personnel.

Privacy breaches can be potentially serious and a failure to respond appropriately may result in a breach of Australian Principle of Privacy and WA health records legislation with associated financial and reputational damage.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* requires that data breaches be reported to both any individuals at risk of serious harm and the office of the Australian Information commissioner (OAIC)

A data breach is required to be reported to the OAIC if the loss of information is such that it is likely to result in serious harm (physical, psychological, emotional, financial, reputational) to the individuals whose personal information was affected. As such there are three criteria that need to be fulfilled in order for a breach to be notifiable.

1. There needs to be a loss, unauthorised access or unauthorised disclosure of personal information. This may include financial, tax file numbers, identity information or contact information.
2. The loss of this information must be likely to result in serious harm to one or more individuals
3. Remedial action did not remove the likely risk of serious harm

The presence of the likelihood of serious harm is based on an objective assessment, from the viewpoint of a reasonable person in the School's position (rather than the individual to whom the information relates).

Response Plan

If a privacy breach occurs or is suspected, School personnel must adhere to the process set out below (as described in the *Officer of the Australian Information Commisioner'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 be sought if necessary.

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

1) School personnel who become aware of the suspected breach will report this to the principal as soon as possible and at a maximum within 24 hours. If known, the following information should be provided:
    a. When the breach occurred (time and date)
    b. The type of personal information involved
    c. The cause of the breach
    d. How the breach was discovered
    e. Which systems were affected

f. The individuals involved
g. Any corrective actions that have taken place to resolve or contain the breach

Immediate steps should be taken to identify and contain the Data Breach, such as retrieval of personal information, ceasing unauthorised access or shutting down or isolating the affected system, as well as other steps to mitigate or remediate the harm any individual could suffer from the Data breach. Evidence from the Data Breach should be preserved as this may be valuable in determining its cause.

For breaches occurring outside of the school e.g. from a contractor or online service, there will need to be a determination of who is to notify the OAIC and affected individuals which should be stipulated in the contract. As such this is unlikely to be notifiable on the part of the School however an assessment of the factors leading to the data breach, the risk of harm and the need for preventive measures should still be done. The school reserves the right to take additional steps if their assessment of risk differs from that of the contractor.

2) A preliminary assessment will be done to determine if a privacy data breach has occurred and how severe (low, medium, high) this is likely to be. A privacy data breach will be found to have occurred where there was unauthorised access or disclosure of personal or sensitive information, or personal or sensitive information was lost and unauthorised access was likely to occur.
   The severity of the breach will involve assessment of the following information:
   - Type and extent of personal information involved
   - Number of individuals affected
   - The presence of any security measures and the likelihood that these could overcome e.g. the presence of an encryption key to circumvent encryption technology
   - The person or kinds of people who could possibly now have access to the data
   - The likelihood that the person who has, or could, obtain the information has the knowledge required to circumvent the security technology or methodology
   - The risk of serious harm to the affected individuals, including physical, physiological, emotional, economic/financial or reputational harm.
   - If corrective action was taken the likelihood that there was access, disclosure or loss prior to this occurring
   - The possibility of media or stakeholder attention

The following table sets out examples of the different risk levels.

Risk level	Description	Reason for judgement
High	Large sets of personal information or highly sensitive personal 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	Near miss or potential event occurred. No identified loss, misuse or interference of personal

		information

Consultation with staff or experts (e.g. cyber security experts) should be done if needed.

Data breaches judged to be at medium or high risk or if there is a possibility of media or stakeholder attention, need to be dealt with by the Data Breach response team. The Principal must also consider if any of the affected individuals should be notified immediately where serious harm is likely.

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 takes any further steps not already done in phase to contain the Data Breach and mitigate or remediate harm to affected individuals.
2) The response team works to evaluate the risks associated with the data breach including by:
    i. Identifying the type of personal information (e.g. financial, tax file numbers, identity information, contact information) involved in the Data Breach
    ii. Identifying the date, time, duration, and location of the Data Breach
    iii. Establishing who could have access to the personal information
    iv. Establishing the number of individuals affected
    v. Establishing who the affected, or possibly affected, individuals are.
    vi. Establishing how successful attempts to mitigate the risk have been

3) Whether the Data Breach is notifiable is determined by assessment of factors in appendix 2 If the Data Breach is considered likely to cause serious harm to any individual affected, it is a notifiable data breach for the purpose of mandatory reporting to the OAIC.
4) All reasonable steps must be taken to ensure the assessment in completed as soon as possible and in any event within 30 days.

Phase 3: Consider Data Breach notification

1) The Principal must prepare a prescribed statement in accordance with the *OAIC Notifiable Data Breach Statement-Form* and provide a copy to the OAIC within 30 days of becoming aware of the breach.

2) Unless the breach involves another organisation and the other organisation is taking responsibility for these notifications or where the OAIC makes a declaration that the school is not required to comply with the notification requirements or may delay giving notice, individuals affected must be notified either directly or indirectly.
    a. Individuals to whom information in the breach belonged or individuals at risk of serious harm from the breach must be notified if practical to do so. This can be done by any reasonable method e.g. call, SMS, physical mail, social media post or in-person communication. If the individual affected is a student, the parent or

guardian will likely need to be informed in addition to the student. The notification must include:

i. The identity and contact details of the school
ii. A description of the breach and the organisation that has reasonable grounds to believe the breach occurred
iii. The kind of information concerned
iv. Recommendations about the steps that individuals should take in response to the breach

b. If it is not practical to inform affected individuals directly, they must be informed indirectly via publishing of the statement provided to the OAIC, including on the school website. Reasonable steps must be taken to publicise these contents.

Phase 4. Take action to prevent future Data Breaches

1) Any steps from phase 2, that were not completed due to causing a delay in proceeding to phase 3 should be completed now.
2) The Principal must enter details of the Data Breach and response taken into a Data Breach log. This should be reviewed yearly to identify any reoccurring data breaches.
3) The Board Chair, will identify an appropriate individual to 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 school board will assess the review and re-evaluate the privacy policy in view of the incident, to determine a prevention plan if necessary. An audit of the school privacy policy and processes as well as other relevant processes may be ordered by the board.

Response team

Principal

- Decide on Remedial Action following a data breach
- Implement training for staff on privacy
- Oversee response plan
- Communicate with relevant parties
- Notify relevant parties where data breach has occurred

Business Manager

- Investigation/assessment of data breach
- Liaise with staff to implement mitigating strategies

IT Support

- Investigating electronic data breach
- Installation of IT strategies to mitigate data breach

Associated Policy

Record Management Policy

Information and Communication Technology Use Policy

Related Source Documents:

1. Australian Privacy Principles, Privacy Act 1988, Schedule 1
2. National Catholic Education Commission and Independent Schools Council of Australia. Privacy Compliance Manual. November 2019.
3. Australian government. Office of the Australian Information Commissioner. Guide to securing personal information. 5 June 2018. Oaic.gov.au/privacy/guidelines-and-advice/guide-to-securing-personal-information
4. Australian government. Office of the Australian Information Commissioner. Data breach preparation and response. July 2019. Oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/

Appendix 1

Summary of a School's obligations imposed by the Australian Privacy Principles

1. Manage personal information in an open or transparent way
2. Take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the school's functions or activities that:
    a. Will ensure compliance with the APP
    b. Will enable the School to deal with inquiries or complaints about compliance with the APPs
3. Have a clearly expressed and up to date privacy policy about the School's management of personal information
4. If it is lawful or practicable, give individuals the option of interacting anonymously with the School or using a pseudonym
5. Only collect personal information that is reasonably necessary for the School's functions or activities
6. Obtain consent to collect sensitive information unless specified exemptions apply
7. Use fair and lawful means to collect personal information
8. Collect personal information directly from an individual if it is reasonable and practicable to do so
9. If the school receives unsolicited personal information, determine whether it could have collected the information under APP 3 as if it had solicited the information. If so APPs 5-13 will apply. If not, the information must be destroyed or de-identified.
10. At the time the School collects personal information or as soon as practicable afterwards, take such steps (if any) as are reasonable in the circumstances to make an individual aware of:
    a. Why the school is collecting information about them
    b. Who else the school might give it to
    c. Other specified matters
11. Take such steps (if any) as are reasonable in the circumstances to ensure the individual is aware of this information even if the School has collected it from someone else
12. Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in APP 6.2 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances).
13. If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.
14. Do not use personal information for direct marketing, unless one of the exceptions in APP 7 applies (for example, the School has obtained consent or where the individual has a reasonable expectation of their information being used or disclosed for that purpose and the School has provided a simple means for the individual to unsubscribe from such communications).

15. Before the School discloses personal information to an overseas recipient it must take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs, unless an exception applies
16. Government related identifiers must not be adopted, used, or disclosed unless one of the exceptions applies (e.g. the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the School's functions or activities)
17. Take such steps (if any) as are reasonable in the circumstances to ensure the personal information the School collects, uses or discloses is accurate, complete and up to date. This may require the school to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.
18. Take such steps as are reasonable in the circumstances to protect the personal information the School holds from misuse, interference, and loss and from unauthorised access, modification or disclosure.
19. Take such steps as are reasonable in the circumstances to destroy or permanently de-identify personal information no longer needed for any purpose for which the school may use or disclose the information.
20. If requested, the School must give access to the personal information it holds about an individual unless circumstances apply that allow it to limit the extent to which it gives access.

Note: This is a summary only and not a full statement of obligations.

Appendix 2: Data breach risk assessment factors

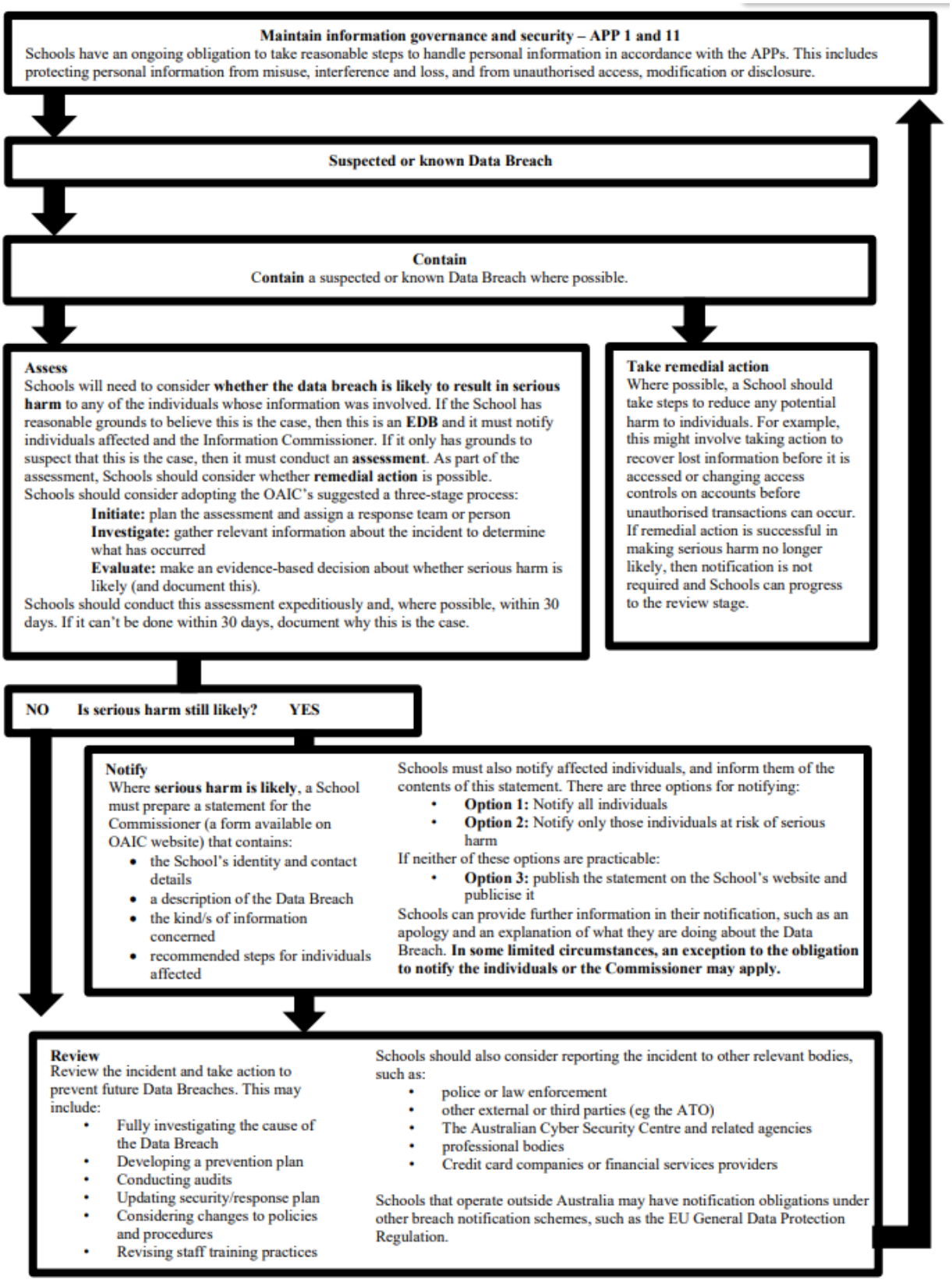
Who the personal information is about	
Who is affected by the breach?	Are students, parents, staff, contractors, service providers and/or other agencies or organisations affected? E.g. Disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information
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 if compromised A combination of personal information may also pose a greater risk of harm
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 students who attend the School may not give rise to significant risk. However, the same information about students with disabilities may be more likely to cause harm. The disclosure of names and addresses of students 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 example, if a teacher at another school gains unauthorised access to a student's name and address without malicious intent (e.g. by being accidentally emailed) the risk of serious harm to the student may be unlikely.
Have there been other breaches that could have a cumulative effect?	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.
How could the personal information be used?	Consider the purposes for which the information could be used. Could it be used to commit identity theft, financial fraud, abuse the individual physically or emotionally (including to humiliate the affected individual and social and workplace bullying)? E.g. information on students' domestic circumstances

	may be used to bully or marginalise the student 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?
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 on (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 note easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in a 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 (e.g. 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 bene found and 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 compromised 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 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.
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)
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 students who attend the school may not be sensitive information, however the same information about students with disabilities may be.
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 other people likely could not iii) Information that has been adequately destroyed and cannot be retrieved to its original form
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 these 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 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 student'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.
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?	Example 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.
Risk of other harms	
What other possible harms could result from the breach, including harms to the School?	Examples include loss of public trust in the School, 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, breach of secrecy provisions in the applicable legislation.

Appendix 3: Data breach process



Modified version of the OAIC data breach response summary available at www.oaic.gov.au/privacylaw/privacy-act/notifiable-data-breaches-scheme