# Executive Summary

Mooroolbark Grammar is required to comply with privacy laws that are designed to protect the personal information of individuals.

Compliance with our privacy obligations is important because the people the School deals with (including students and parents) expect us to handle their personal information properly. There are different types of personal information including sensitive information and health information. Failure to comply with privacy laws can cause harm to students and their parents, particularly if sensitive or health information is disclosed without their consent.

As a key part of our compliance obligations we have developed a Privacy Policy that is published on our public website and outlines the circumstances in which we collect personal information, how we use and disclose that information and how we manage requests to access and/or change that information.

We have also appointed a Privacy Officer who is responsible for managing privacy queries and complaints as well as privacy breaches. is our Privacy Officer.

The School has a legal obligation to report certain data breaches to the Office of the Australian Information Commissioner (OAIC). A privacy data breach can take many forms and have many causes. The breach may involve human error, a system fault or a deliberate hacking of a database.

To determine whether a data breach has occurred we use a Guide to Data Breach Identification.

In the event a data breach has occurred we manage the breach in accordance with our Data Breach Response Plan.

Information sharing regimes under state/territory legislation relating to child protection override the privacy requirements under the Privacy Act.

For more information, refer to our Child Safety Program.

# Our Privacy Policy

In the course of Mooroolbark Grammar's activities, we manage and protect personal information in accordance with the Privacy Act 1988 (Cth) (Privacy Act) and the 13 Australian Privacy Principles (APPs) as well as the requirements of the Health Records Act (Vic).

**Scope of Policy**

This Policy outlines the circumstances in which we obtain personal information, how we use and disclose that information and how we manage requests to access and/or change that information.

**How We Collect Personal Information**

Personal information is information, or an opinion about an individual, from which they can be reasonably identified. Depending on the circumstances, we may collect personal information from the individual in their capacity as a student, contractor, volunteer, stakeholder, job applicant, alumni, visitors or others that come into contact with the School.

In the course of providing services we may collect and hold:

- **Personal Information** including names, addresses and other contact details; dates of birth; next of kin details; photographic images; attendance records and financial information.
- **Sensitive Information** (particularly in relation to student and parent records) including government identifiers (such as TFN), religious beliefs, nationality, country of birth, professional memberships, family court orders and criminal records.
- **Health Information** (particularly in relation to student and parent records) including medical records, disabilities, immunisation details and psychological reports.

**As part of our recruitment processes for employees, contractors and volunteers, we may collect and hold:**

- **Personal Information** including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation, media, directorships, property ownership and driver's licence information.
- **Sensitive Information** including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders and criminal records.

- **Health Information** (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

Generally, we will seek consent from the individual in writing before we collect their sensitive information (including health information).

It is noted that employee records are not covered by the APPs where they relate to current or former employment relations between the School and the employee.

However, a current or former employee's health records are covered by the Victorian Health Privacy Principles.

**Collection of Personal Information**

The collection of personal information depends on the circumstances in which Mooroolbark Grammar is collecting it. If it is reasonable and practical to do so, we collect personal information directly from the individual.

**Solicited Information**

Mooroolbark Grammar has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form or Health Information Disclosure Form). However, given the nature of our operations we may also receive personal information by email, letters, notes, via our website, over the telephone, in face-to-face meetings, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g. a third-party administrator, referees for prospective employees) or independent sources. However, we will only do so where it is not reasonable and practical to collect the personal information from the individual directly.

**Information Collected from Our Website**

We may collect information based on how individuals use our website. We use "cookies" and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic. We do not use this information to personally identify individuals.

**Unsolicited information**

Mooroolbark Grammar may be provided with personal information without having sought it through our normal means of collection. This is known as “unsolicited information” and is often collected by:

- misdirected postal mail – letters, notes, documents
- misdirected electronic mail – emails, electronic messages
- employment applications sent to us that are not in response to an advertised vacancy
- additional information provided to us which was not requested.

Unsolicited information obtained by Mooroolbark Grammar will only be held, used and or disclosed if it is considered as personal information that could have been collected 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 personal information as appropriate.

**Collection and Use of Sensitive Information**

We only collect sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and we have the individual’s consent
- necessary to lessen or prevent a serious threat to life, health or safety
- another permitted general situation
- another permitted health situation.

We may share sensitive information to other entities in our organisation structure, but only if necessary, for us to provide our products or services.

**How do we use personal information?**

Mooroolbark Grammar only uses 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 for an activity or purpose to which you have consented.

Our primary uses of personal information include, but are not limited to:

- 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 the activities of School associations

- supporting the activities of the School
- 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
- the employment of staff
- the engagement of volunteers.

We will only use or disclose sensitive or health 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.

We may share personal information to related bodies corporate, but only if necessary, for us to provide our services.

The School may disclose information about an individual to overseas recipients only when it is necessary, for example to facilitate a student exchange program. The School will not however send information about an individual outside of Australia without their consent.

**Storage and Security of Personal Information**

Mooroolbark Grammar stores Personal Information in a variety of formats including, but not limited to:

- databases
- hard copy files
- personal devices, including laptop computers
- third party storage providers such as cloud storage facilities
- paper based files.

Mooroolbark Grammar takes all reasonable steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- restricting access and user privilege of information by staff depending on their role and responsibilities

- ensuring staff do not share personal passwords
- ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. staff access is subject to user privilege
- ensuring access to Mooroolbark Grammar's premises is secured at all times.
- implementing physical security measures around the School buildings and grounds to prevent break-ins
- ensuring our IT and cyber security systems, policies and procedures are implemented and up to date
- ensuring staff comply with internal policies and procedures when handling the information
- undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the apps or a similar privacy regime
- the destruction, deletion or de-identification of personal information we hold that is no longer needed or required to be retained by any other laws.

Our public website may contain links to other third-party websites outside of Mooroolbark Grammar.

Mooroolbark Grammar is not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

**Responding to Data Breaches**

Mooroolbark Grammar will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC). For more information refer to Notifiable Data Breaches.

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

**Disclosure of Personal Information**

Personal information is used for the purposes for which it was given to Mooroolbark Grammar, or for purposes which are directly related to one or more of our functions or activities.

Personal information may be disclosed to government agencies, other parents, other schools, recipients of School publications, visiting teachers, counsellors and coaches, our services providers,

agents, contractors, business partners, related entities and other recipients from time to time, if the individual:

- has given consent; or
- would reasonably expect the personal information to be disclosed in that manner.

Mooroolbark Grammar may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- we are required to do so by law
- the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety
- another permitted general situation applies
- disclosure is reasonably necessary for a law enforcement related activity
- another permitted health situation exists.

**Disclosure of Personal Information to Overseas Recipients**

Personal information about an individual may be disclosed to an overseas organisation in the course of providing our services, for example when storing information with a “cloud service provider” 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)
- we have satisfied ourselves that the overseas recipient is compliant with the APPs, or a similar privacy regime
- 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
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

**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 Mooroolbark Grammar 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.

**The Quality of Personal information**

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.

If the School becomes aware that the personal information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

**Access and Correction of Personal Information**

You may submit a request to us to access the personal information we hold, or request that we change the personal information. Upon receiving such a request, we will take steps to verify your identity before granting access or correcting the information.

If we reject the request, you will be notified accordingly. Where appropriate, we will provide the reason/s for our decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and we will attach this to their record.

**Complaints**

You can make a complaint about how the School manages personal information, including a breach of the APPs by notifying us in writing as soon as possible. We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we may seek further information in order to provide a full and complete response.

Mooroolbark Grammar does not charge a fee for the handling of complaints.

If you are not satisfied with our response, you may refer the complaint to the OAIC. A complaint can be made using the OAIC online Privacy Complaint form or by mail, fax or email.

A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

**How to Contact Us**

The School can be contacted about this Privacy Policy or about personal information generally, by:

- Emailing gabriella@mooroolbarkgrammar.vic.edu.au
- Calling 0439 008 091
- Writing to our Privacy Officer at admissions@mooroolbarkgrammar.vic.edu.au or 4 Birchwood Drive, Mooroolbark, Vic

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. 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 public website regularly for any changes.

This Privacy Policy was last reviewed:

# Notifiable Data Breaches

A data breach can take many forms and have many causes. The breach may involve human error, a system fault or a deliberate hacking of a database. Depending on the circumstances of the incident, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference.

Our legal obligations for reporting an incident can vary depending on the circumstances of the incident.

Mooroolbark Grammar has established the following work systems, practices, policies and procedures for responding to and reporting suspected and actual data breaches both internally and externally. This includes:

- Terminology
- Guide to Data Breach Identification
- Remedial Action
- Data Breach Response Plan

The Guide to Data Breach Identification is designed to assist our staff in making decisions with respect to identifying different data breaches and when a breach will be a Notifiable Data Breach.

The Privacy Officer must be notified of any data breach.

**Terminology**

Data Breach

It is important to note that although the Privacy Act regulates the handling of personal information, not "data", the OAIC uses the term data breach rather than "personal information security breach" in its guidance to organisations on how to respond to an incident.

A data breach occurs when personal information held by Mooroolbark Grammar is misused, interfered with, lost or subject to unauthorised access, modification or disclosure. In other words, a data breach may occur as a result of a failure by Mooroolbark Grammar to protect the security of:

- personal information, in accordance with APP 11: Security of Personal Information; and/or
- credit information, in accordance with the Privacy Act and Credit Reporting Code.

Examples of data breaches include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- databases containing personal information being 'hacked' or otherwise illegally accessed by individuals outside of the School
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- the School mistakenly providing personal information to the wrong person, for example by sending details to the wrong address.

Data breaches that are likely to result in serious harm to any of the individuals to whom the information relates may be a Notifiable Data Breach.

Likely means ‘more probable than not’.

Notifiable Data Breach

A Notifiable Data Breach occurs where the School holds personal information relating to one or more individuals, is required to ensure the security of that personal information, and:

- there is unauthorised access to or disclosure of information, and a reasonable person would conclude that this would be likely to result in serious harm to any of the individuals to whom the information relates; or
- information is lost in circumstances where unauthorised access to or disclosure of information is likely to occur, and a reasonable person would conclude that, assuming this were to occur, it would be likely to result in serious harm to any of the individuals to whom the information relates.

Under the Privacy Act, these types of data breaches are referred to as “eligible data breaches”, however for the purposes of this policy, the School has adopted the phrase Notifiable Data Breach as in the OAIC's guidance materials.

Serious Harm

This term is not defined in the Privacy Act. The term could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

The Act sets out a list of factors to consider when determining whether a reasonable person would conclude that an incident of access to, or a disclosure of, information:

- would be likely; or
- would not be likely,

to result in serious harm to any of the individuals to whom the information relates.

Those factors are:

- the kind/s of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information

- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that the persons, or the kinds of persons, who:
    - have obtained or, or who could obtain the information
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates
- have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

**Remedial Action**

What is remedial action?

Remedial action is action taken to contain a suspected data breach and to prevent the likely risk of serious harm occurring.

For example, if a staff member accidentally sends an email containing personal information to the wrong recipient, the Privacy Officer and the staff member may be able to take action to remedy the breach so that a reasonable person would conclude that the breach would likely not result in serious harm to any person to whom the information relates. Action could include recalling the email or contacting the recipient who agrees to delete the email.

Successful Remedial Action

If remedial action is successful, and the likely risk of serious harm occurring has been prevented, the breach will not amount to a Notifiable Data Breach and notification to the OAIC and affected individuals will not be required.

Unsuccessful Remedial Action

If remedial action is unsuccessful, meaning that the likely risk of serious harm occurring has not been prevented, the data breach will be a Notifiable Data Breach and, it may be appropriate for the Privacy Officer to escalate the matter to the Data Breach Response Team.

**Voluntary Notification to OAIC and/or Individuals**

Not all data breaches require notification to the OAIC and affected individuals. If there are reasonable grounds to suspect that there may have been a Notifiable Data Breach, we must comply with the notification requirements set out in the Privacy Act.

If a data breach is not a Notifiable Data Breach, the School is not legally required to notify the OAIC and affected individuals but may choose to do so as a matter of best practice. A decision to voluntarily notify the OAIC and/or affected individuals will be made on a case-by-case basis having regard to the following factors:

- notification as a reasonable security safeguard: to help protect information from misuse, interference or loss
- notification as openness about privacy practices: being open and transparent when something goes wrong
- notification as restoring control over personal information: where it will assist individuals to regain control of the information
- notification as a means of rebuilding public trust, where it will demonstrate to the public that the School takes its privacy obligations seriously

OAIC Contact Details

If we decide to notify the OAIC we will do so using one of the following contact options:

- Email: enquiries@oaic.gov.au
- Telephone: 1300 363 992
- Facsimile: + 61 2 9284 9666
- Post: GPO Box 5218, Sydney NSW 2001

**Data Breach Response Plan**

If a data breach is identified using the Guide to Data Breach Identification the Data Breach Response Plan must be followed.

The Data Breach Response Plan sets out procedures and clean lines of authority for the School in the event that it experiences circumstances that amount to a data breach or a Notifiable Data Breach.

The response in the Data Breach Response Plan is intended to enable the School to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals and to meet our notification obligations under the Privacy Act.

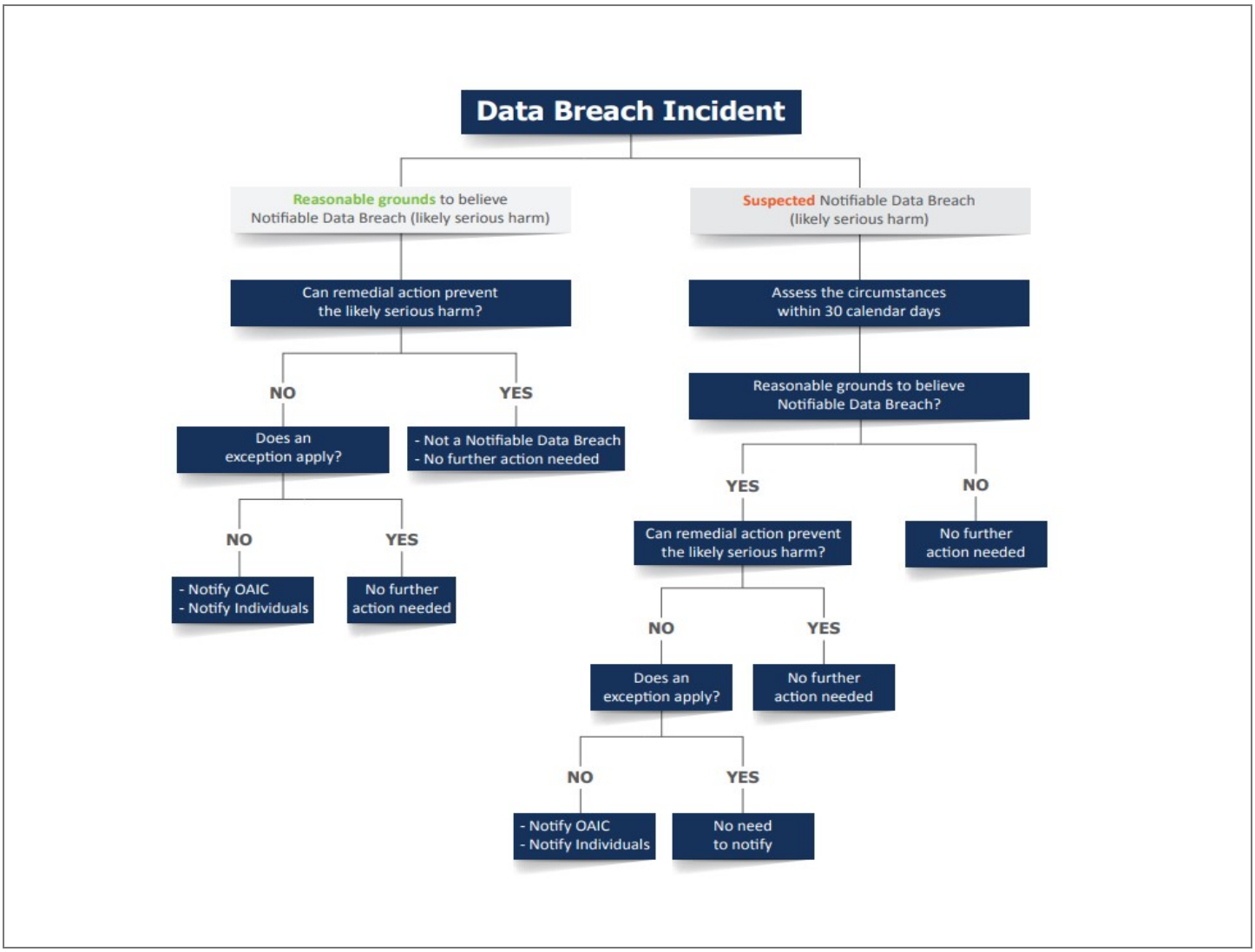
**Information Collecting**

Various steps in the Data Breach Response Plan require the collection of information.

In the event that the Data Breach Response Plan is activated, the Privacy Officer will ensure that:

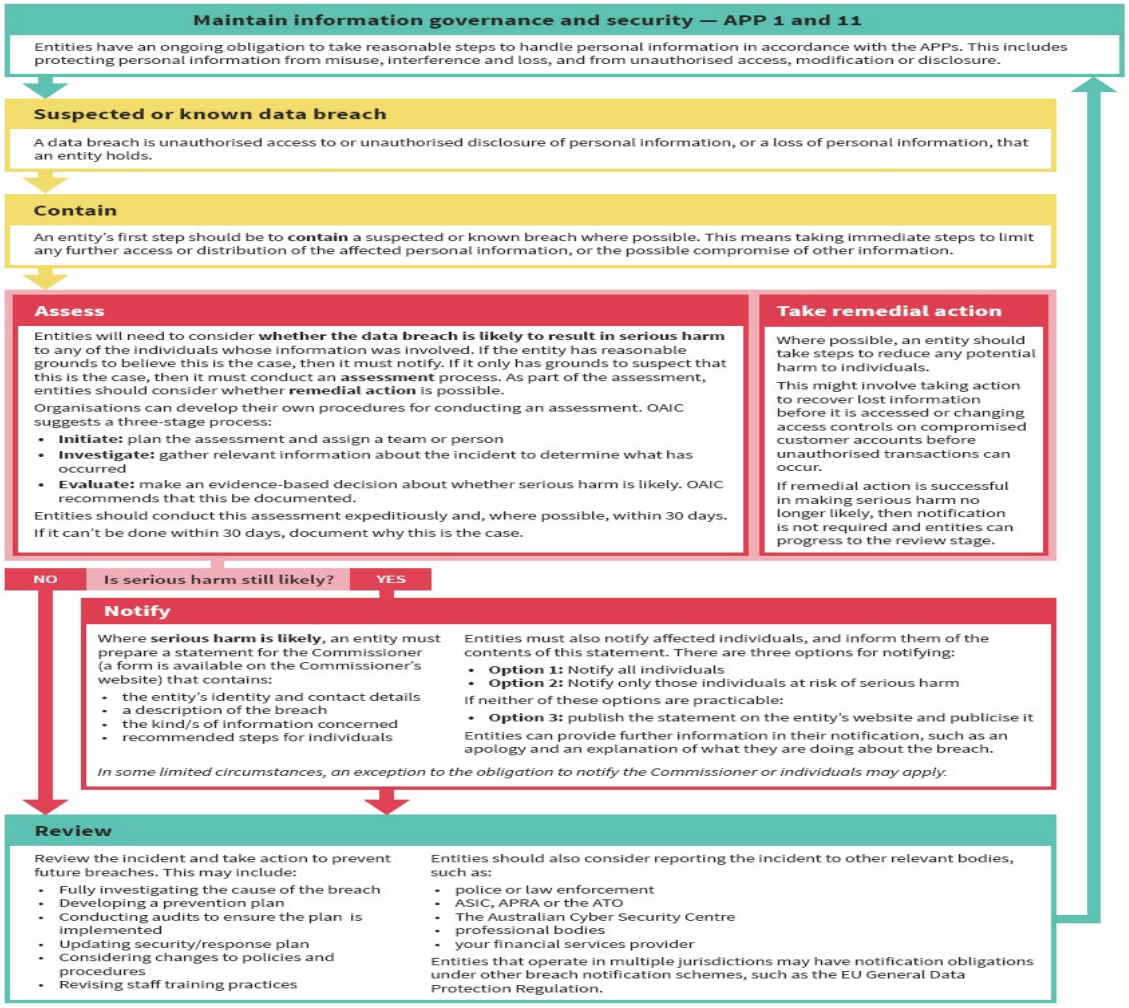
- evidence is preserved that may be valuable to determine the context of the data breach and a list of affected individuals, or possible affected individuals
- information will be compiled for external notification processes and internal reporting
- records of the information are kept.

## Guide to Data Breach Identification




## Data Breach Response Plan

The OAIC has provided the following Data Breach Response Plan that the School uses:


Maintain information governance and security — APP 1 and 11
Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
Suspected or known data breach
A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.
Contain
An entity's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.
Assess
Entities will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an assessment process. As part of the assessment, entities should consider whether remedial action is possible.
Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:
Initiate: plan the assessment and assign a team or person
Investigate: gather relevant information about the incident to determine what has occurred
Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.
Entities should conduct this assessment expeditiously and, where possible, within 30 days.
If it can't be done within 30 days, document why this is the case.
Take remedial action
Where possible, an entity should take steps to reduce any potential harm to individuals.
This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.
If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.
NO
Is serious harm still likely?
YES
Notify
Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:
the entity's identity and contact details
a description of the breach
the kind/s of information concerned
recommended steps for individuals
Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:
Option 1: Notify all individuals
Option 2: Notify only those individuals at risk of serious harm
If neither of these options are practicable:
Option 3: publish the statement on the entity's website and publicise it
Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.
In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.
Review
Review the incident and take action to prevent future breaches. This may include:
Fully investigating the cause of the breach
Developing a prevention plan
Conducting audits to ensure the plan is implemented
Updating security/response plan
Considering changes to policies and procedures
Revising staff training practices
Entities should also consider reporting the incident to other relevant bodies, such as:
police or law enforcement
ASIC, APRA or the ATO
The Australian Cyber Security Centre
professional bodies
your financial services provider
Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.