PRIVACY POLICY

PURPOSE

Newmark Primary (the school) is required to comply with privacy laws that are designed to protect the personal information of individuals.

PRINCIPLES

- Students, parents/carers and staff, trust the school to handle personal information responsibly.
- Failure to comply with privacy laws can cause harm to students, parents/carers or staff, particularly if sensitive or health information is disclosed without consent.
- Strong privacy systems and processes will safeguard the protection of personal information collected by the school.

AIMS

As a key part of the compliance obligations the school has developed a Privacy Policy that is published on our website and outlines the circumstances in which:

- the school collects personal information;
- how the school uses and discloses that information; and
- how the school manages requests to access and/or changes that information.

LEGAL AND REGULATORY BASIS FOR COMPLIANCE

- Privacy Act 1988 (Cth) (Privacy Act)
- 13 Australian Privacy Principles (APPs)
- Health Records Act (Vic)
- Education and Training Reform Act 2006 (Vic)
- Education and Training Reform Regulations (2017)
- Victorian Registration and Qualifications Authority (VRQA) Minimum Standards

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

KEY DEFINITIONS

Australian Privacy Principle (APP) 1.3 requires an APP entity (an organisation) to have a clearly expressed and up-to-date APP Privacy Policy describing how it manages personal information.

Privacy Act The Privacy Act 1988 was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an

annual turnover of more than $3 million, and some other organisations, handle personal information.

OAIC Office of the Australian Information Commissioner responsible for adherence to the Privacy Act.

Personal Information is information, or an opinion about an individual, from which they can be reasonably identified.

Unsolicited information is information the school may be provided with personal information without having sought it through our normal means of collection.

Primary purpose of personal information include, but is 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/carers informed as to school community matters through correspondence;
- 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 the school to improve daily operations, including training staff;
- systems development, developing new programs and services, undertaking planning, research and statistical analysis;
- school administration including for insurance purposes;
- the employment of staff; and
- the engagement of volunteers.

Data breach occurs when personal information held by the school 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 the school 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.

Notifiable Data Breaches are data breaches that are likely to result in serious harm to any of the individuals to whom the information relates.

Serious Harm 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 Privacy 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.

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

SCOPE

This policy outlines the circumstances in which the school obtains personal information, how the school uses and discloses that information, and how the school manages requests to access and/or change that information.

Depending on the circumstances, the school may collect personal information from the individual in their capacity as a student, contractor, volunteer, stakeholder, job applicant, alumni, visitor or other that come into contact with the school.

In the course of providing educational services the school may collect and hold:

- personal information including names, addresses and other contact details, dates of birth, next of kin details, photographic images, professions, attendance records and financial information;
- sensitive information (particularly in relation to student and parent records) including government identifiers, nationality, country of birth, family court orders and criminal records; and/or
- health information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details and psychological reports.

As part of the school's recruitment processes for staff, contractors and volunteers, the school may collect and hold:

- personal information including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation (e.g. VIT), working with children checks, directorships 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; and/or
- health information (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

The application of the policy is relevant to the school board, principal, and to prospective, current and past staff, students and parents/carers.

ROLES AND RESPONSIBILITIES

The **school board** is responsible for:

- reviewing and endorsing the Privacy Policy

The **principal** is responsible for:

- establishing school Privacy Policy;
- ensuring robust protocol to address any data breach, including assessment of any Notifiable Data Breach; and
- together with the Business Manager, assessing data breaches and whether these amount to Notifiable Data Breach (reportable to OAIC).

The **business manager** is responsible for:

- ensuring personal information is protected and deals with issues relating to how the school handles the privacy of students, parents/carers and staff; and
- managing privacy queries and complaints as well as privacy breaches.

The **staff** are responsible for:

- safeguarding the privacy of student, parent/carers and staff personal information;
- accessing personal information only relevant to effectively complete their work; and
- safely archiving and/or disposing personal information not required by the school (see Record Management Policy for procedures on how to safely dispose of information).

The **parents/carers** are responsible for:

- providing and maintaining personal information relating to them and their child/ren that is correct and up-to-date.

The **students** are responsible for:

- ensuring they secure school devices and personal documents.

PROCEDURES

Collection of Personal Information

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

The school has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Agreement or Health Information Disclosure Form). However, given the nature of our operations the school 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.

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

Unsolicited information obtained by the school 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 the school will

destroy, permanently delete or de-identify the personal information as appropriate. Examples of unsolicited information include, but is not limited to:

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

Information Collected from our Website

The school may collect information based on how individuals use the website. The school uses ''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 the website. This information is collected to analyse and improve the website, marketing campaigns and to record statistics on web traffic. The school does not use this information to personally identify individuals.

Collection and Use of Sensitive Information

The school only collects sensitive information if it is:

- reasonably necessary for one or more of the school functions or activities, and with the individual's consent;
- necessary to lessen or prevent a serious threat to life, health or safety;
- another permitted general situation; and/or
- another permitted health situation.

The school may share sensitive information with other entities in the organisation structure, but only if necessary, for the school to provide products or services.

How the School Uses Personal Information

The school only uses personal information that is reasonably necessary for one or more of the school's functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected, or for an activity or purpose to which the school has received consent.

The school will only use or disclose sensitive or health information for a secondary purpose if it is reasonable to expect the school to use or disclose the information and the secondary purpose is directly related to the primary purpose.

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 consent.

Storage and Security of Personal Information

The school stores personal information in a variety of formats including, but not limited to:

- databases;
- hard copy files;
- personal devices, including laptop computers; and

- third party storage providers such as cloud storage facilities, paper based files.

The school takes all reasonable steps to protect the personal information it holds 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 the school's premises is secured at all times;
- implementing physical security measures around the school buildings and grounds to prevent break-ins;
- ensuring the 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 authorised third party service providers who may have access to personal information, including school administration system providers and cloud service providers, to ensure as far as practicable that they are compliant with the APPs or a similar privacy regime; and
- the destruction, deletion or de-identification of personal information the school holds that is no longer needed or required to be retained by any other laws.

The school's public website may contain links to other third-party websites outside of the school. The school is not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

Disclosure of Personal Information

Personal information is used for the purposes for which it was given to the school, or for purposes which are directly related to one or more of the school's functions or activities.

Personal information may be disclosed to government agencies, other parents/carers, other schools, recipients of school publications, visiting teachers, counsellors and coaches, 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.

The school 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; or

- 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 services, for example when storing information with a "cloud service provider" which stores data outside of Australia.

The school will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless the school:

- has the individual's consent (which may be implied);
- is satisfied that the overseas recipient is compliant with the APPs, or a similar privacy regime;
- forms 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;
- is 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.

The school takes 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. The school will treat notices provided to parents/carers as notices provided to students, and will treat consents provided by parents/carers as consents provided by a student.

The school is 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. The school also acknowledges 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
The school takes all reasonable steps to ensure the personal information it holds, uses and discloses 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, the school will take reasonable steps to rectify the incorrect or out of date information.

Access and Correction of Personal Information
The school will receive requests to access the personal information it holds, or requests that it changes the personal information. Upon receiving such a request, the school will take steps to verify the identity of the person making the request before granting access or correcting the information.

If the school rejects the request, where appropriate, the school will provide the reason/s for the decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and the school will attach this to their record.

Responding to Data Breaches
The school will take appropriate, prompt action if it has 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).

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; and
- the school mistakenly providing personal information to the wrong person, for example by sending details to the wrong address.

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

Wherever possible the school will take remedial actions to contain a suspected data breach. For example, if a staff member accidentally sends an email containing personal information to the wrong recipient, the principal (or delegate) 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 contacting the recipient who agrees to delete the email.

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.

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 Business Manager to escalate the matter to the Data Breach Response Team.

Notifiable Data Breaches

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.

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.

The school's legal obligation for reporting an incident can vary depending on the circumstances of the incident.

If a suspected and actual data breach occurs, the school will follow the guidelines set out in the 'Data Breach Preparation and Response - A guide to managing data breaches in accordance with the Privacy Act 1988'

The Business Manager must be notified of any data breach.

The school has a legal obligation to report certain data breaches to the 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.

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, the school will comply with the notification requirements set out in the Privacy Act.

RELATED POLICIES

- Record Management Policy
- Technology Policy
- Enrolment Policy
- Complaints Policy

SUPPORTING DOCUMENTS

- Enrolment Agreement
- Permissions and Consent Forms
- Register of Students Medical Conditions

POLICY REVIEW

The school board and principal will review the Privacy Policy every two years, or following a major incident.

ENDORSEMENT

Updated date	January 2023
Endorsed by	School Board
Endorsed on	April 2023