



**MALEK FAHD
ISLAMIC SCHOOL**

Privacy Policy

**Version: V3.0
6 August 2026**

Contents

Policy Custodian:.....	2
Version Control:.....	2
Policy Review	2
Introduction	3
Who We Collect Information From	3
Kinds of Personal Information We Collect.....	3
How We Collect Personal Information	4
National Police Checks.....	5
Information Collected Through School Systems.....	5
Purposes for Which We Collect, Hold, Use and Disclose Personal Information	6
Who We Disclose Personal Information To	7
Artificial Intelligence (AI)	7
How We Store Personal Information.....	8
Marketing and Communications	8
Security of Personal Information.....	9
Access and Correction of Personal Information	9
Consent and Rights of Access to the Personal Information of Students	10
Complaints	11

Policy Custodian:

Business Manager

Version Control:

Version No	Date	Details	Approved by
1.0	1 June 2020	Initial Version	Principal (Bruce Rixon)
2.0	1 October 2020	Revised	Principal (Bruce Rixon)
3.0	6 August 2026	Revised by HR Manager (Fatme Tahsildar); in the absence of a Business Manager. Reviewed by Source Legal.	Principal (Dr Zachariah Matthews)

Policy Review

This policy will be reviewed every three years if not earlier to take account of any changed technology, legislation, expectations or practices. The next review date is August 2029.

Introduction

At Malek Fahd Islamic School, the protection of personal information is guided not only by legal obligations but also by Islamic values. Islam emphasises the importance of trust (amanah), respect for individual dignity, honesty, accountability, and the safeguarding of the rights and privacy of others. As an Islamic educational institution, the School is committed to handling personal information responsibly, ethically, and with due care in a manner that reflects both its faith-based values and its obligations under Australian law.

This Privacy Policy sets out how Malek Fahd Islamic School (ABN: 41 003 864 891) (School) manages personal information and your rights in relation to that information, including how to make a complaint and how the School deals with complaints. In this Privacy Policy, "Parents" means parents, carers and other persons with parental responsibility for a student.

This Privacy Policy is available on the School's website. If you require this Privacy Policy in an alternative format, please contact us using the details set out in the Contact & Complaints section below. The School will endeavour to provide the Privacy Policy in another format where appropriate and reasonable.

The School is bound by the Australian Privacy Principles contained in the Privacy Act 1988 (Cth). In relation to health records, the School is also bound by the Health Privacy Principles contained in the Health Records and Information Privacy Act 2002 (NSW) (HRIPA).

Under the Privacy Act and the HRIPA, the Australian Privacy Principles and Health Privacy Principles do not apply to certain treatment of employee records. Accordingly, 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 the employee.

However, health information about employees that is held for purposes extending beyond the employment relationship, such as records maintained through on-site health services, may remain subject to the Privacy Act and the HRIPA. This Privacy Policy applies to such information accordingly.

Who We Collect Information From

The School collects personal information from students, parents, carers, emergency contacts, prospective families, employees, job applicants, volunteers, contractors, visitors, former students and other individuals who come into contact with the School.

Kinds of Personal Information We Collect

The types of information the School collects includes (but is not limited to) personal information, including health and other sensitive information, about:

- students and Parents before, during and after the course of a student's enrolment at the School and prospective families (including prospective students), including:
 - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
 - parents' education, occupation, language spoken at home, nationality and country of birth;

- health information (e.g., details of disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports and names of doctors);
- results of assignments, tests and examinations;
- conduct and complaint records, or other behaviour notes, and school reports;
- information about referrals to government welfare agencies;
- counselling reports;
- health fund details and Medicare number (collected for the purpose of administering health and first aid services at the School);
- any Family Court orders;
- criminal records (which are treated as sensitive information);
- volunteering information;
- photos and videos at School events; and
- pre-enrolment information provided during the enquiry and application process;
- job applicants, volunteers and contractors, including:
 - name, contact details (including next of kin), date of birth, and religion;
 - information on job application;
 - professional development history;
 - salary and payment information, including superannuation details;
 - health information (e.g., details of disability and/or allergies, and medical certificates);
 - complaint records and investigation reports;
 - leave details;
 - photos and videos at School events;
 - workplace surveillance information;
 - work emails and private emails (when using work email address) and internet browsing history; and
 - criminal history information and National Police Check information (which are treated as sensitive information);
- visitors to the School, including name, contact details, visit purpose, and access control and CCTV records;
- former students, including historical enrolment and academic records retained for legal, archival and administrative purposes; and
- other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.
- Records are retained in accordance with applicable legal and regulatory retention requirements.

How We Collect Personal Information

- **Personal information you provide:** The School generally collects personal information about an individual directly from the individual (or their Parent in the case of students). This includes by way of forms, face-to-

face meetings and interviews, emails and telephone calls.

- **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, a reference from another school or a referee for a job applicant. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.
- **Personal information from other sources:** We may also collect personal information through surveillance activities (such as CCTV security cameras) and email monitoring. CCTV and monitoring activities are conducted for safety, security and compliance purposes. Where required, appropriate notices are displayed in areas subject to CCTV surveillance, and staff are notified of monitoring practices as part of the School's Information and Communication Technology (ICT) policies.

National Police Checks

The School may collect criminal history information through National Police Checks (NPCs) as part of recruitment, child safety and compliance obligations.

Where an NPC is required by law, industrial instrument, or School policy as a condition of an individual's engagement or ongoing role, the provision of NPC information will be requested and treated as a requirement of that position. Where collection is not otherwise legally mandated, the School will seek the individual's consent prior to obtaining an NPC. In all cases, NPC information is treated as sensitive information.

Access is restricted to authorised personnel and information is stored securely in accordance with the School's record management policies and requirements.

NPC information may be collected from prospective employees, existing employees, contractors and volunteers where required by School policy and/or child safety obligations.

Information Collected Through School Systems

The School may also collect personal information through digital and remote learning platforms, including where lessons or other educational sessions are recorded. Such recordings are made only where reasonably necessary for educational purposes, are stored securely, and are deleted when no longer required for that purpose.

Counselling records maintained by the School are personal information and are handled in accordance with this Privacy Policy. Access to counselling records is restricted to authorised personnel on a need-to-know basis. The confidentiality of counselling information may be subject to certain limitations, including where disclosure is required or authorised by law, or where it is necessary to meet child protection obligations (including mandatory reporting requirements) or the School's duty of care to students. Students will be informed of these limits to confidentiality, and the circumstances in which information may need to be shared, before counselling commences.

The School may collect and monitor information generated through the use of School-provided email accounts, student and staff digital accounts, online learning platforms, and BYOD (Bring Your Own Device) devices connected to School networks or systems. Such monitoring is conducted for educational, operational, security, child safety, and compliance purposes in accordance with applicable laws and School policies.

Purposes for Which We Collect, Hold, Use and Disclose Personal Information

The primary purpose for which the School collects, holds, uses and discloses personal information is to enable it to provide educational services to its students and to operate the School effectively.

In relation to students and Parents, the School collects, holds, uses and discloses personal information, including sensitive information, for the following purposes:

- Enrolling and re-enrolling students at the School;
- Providing educational programs, activities and student support services;
- Supporting student health, wellbeing and safety, including administering health care on site, making referrals to external health practitioners and welfare agencies, and complying with mandatory reporting obligations;
- Maintaining and improving the quality and delivery of the School's educational programs and services;
- Reporting on student progress and attendance to Parents and to government authorities;
- Seeking expert advice in relation to legal, medical, child protection, disability and other matters affecting students;
- Complying with legal and regulatory obligations, including duty of care and obligations under child protection, education and equal opportunity legislation;
- Administering the School's financial and administrative functions, including the processing of fees and levies;
- Facilitating the transfer of students to and from the School;
- Community and School communications, including newsletters, publications and promotional materials; and
- Conducting surveys and seeking feedback for the purposes of improving the School's programs and services.

In relation to job applicants, employees, volunteers and contractors, the School collects, holds, uses and discloses personal information, including sensitive information, for the following purposes:

- Assessing suitability for employment, volunteering or engagement with the School;
- Administering employment, engagement and contractor arrangements, including remuneration, leave, performance and conduct management;
- Providing and managing workplace health, safety and wellbeing;
- Complying with legal obligations, including workers' compensation, superannuation, taxation and workplace laws;
- Complying with child protection obligations, including collecting and verifying National Police Check information;
- Managing the School's insurance and risk management arrangements; and
- Administering the School's operations, including ICT, communications and security systems.

Where personal information is intended to be used or disclosed for a purpose other than the primary purpose of collection, the School will take reasonable steps to ensure use or disclosure is consistent with applicable legal

requirements.

Who We Disclose Personal Information To

The School may disclose personal information, including sensitive information, for educational, care and administrative purposes, and to seek support and advice. This may include to:

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student, in accordance with applicable privacy obligations and relevant inter-school information transfer protocols;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers including coaches, volunteers;
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, students with additional needs;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
- people providing administrative and financial services to the School;
- recipients of School publications, such as newsletters and magazines;
- providers of information management, storage and other technology systems and services used by the School, including cloud service providers and student management system providers;
- providers of AI-enabled platforms and tools used by the School for educational and administrative purposes;
- students' Parents or guardians;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Some disclosures may be made to recipients located outside Australia. Please see the section 'How We Store Personal Information' below for further details.

Artificial Intelligence (AI)

The School may use approved AI-enabled platforms and systems to support educational, administrative and operational activities. Where personal information is processed through these systems, the School takes reasonable steps to ensure it is managed securely and in accordance with privacy laws, child safety obligations, and the School's data governance requirements. Staff and student use of AI tools is subject to School policies and approved-platform protocols.

Individuals may request access to or correction of personal information processed through AI systems by contacting the School Principal. The School may update this Privacy Policy as AI technologies and practices evolve.

The School will not knowingly permit personal information to be entered into unapproved public AI platforms where doing so may create privacy, security, confidentiality or child safety risks.

Where collected, Medicare numbers and other government-related identifiers are used and disclosed only for authorised purposes and are not adopted by the School as its own identifiers.

How We Store Personal Information

We store your personal information in hard copy and electronically. We use information management and storage systems provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose of providing services to the School in connection with the systems.

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.

Information may be stored or processed in jurisdictions including Australia, the United States and other countries where approved service providers operate.

The School takes reasonable steps to ensure that overseas service providers handle personal information in accordance with applicable privacy laws. If you would like further information about the overseas locations in which your personal information may be stored or processed, please contact us using the details in the Contact & Complaints section below.

The School retains personal information for the purposes for which it was collected, including to meet any applicable legal, regulatory or archival retention requirements. When personal information is no longer required for those purposes, the School will take reasonable steps to destroy or permanently de-identify it.

Marketing and Communications

The School may use photographs, videos and other information in newsletters, publications, secure online platforms, social media, promotional materials and community communications to celebrate and promote School activities and achievements.

Before publishing photographs or videos of students, the School will seek and manage consent in accordance with its enrolment and consent processes. In determining whether to publish images online, the School will consider privacy, child safety, and online safety risks, including the potential misuse of images through artificial intelligence, deepfake technology, image manipulation, and unauthorised sharing.

The School may limit the publication of student or staff images, names, locations, or other identifying information where doing so is necessary to protect privacy, safety, or wellbeing. The School also encourages parents and carers to carefully consider the risks associated with sharing photographs of children online.

Individuals (or Parents on behalf of students) may update or withdraw their consent for the use of photographs or videos at any time by contacting the School's Privacy Officer using the details in the Contact and Complaints

section below. The School's Privacy Officer is the Business Manager, unless otherwise advised by the School.

From time to time, the School may use personal information to communicate with members of the School community regarding fundraising activities, events, and opportunities to support the School and its programs. The School will only do so where permitted by applicable privacy legislation. Individuals may opt out of receiving fundraising or direct marketing communications at any time by contacting the School's Privacy Officer.

Parents and visitors attending School events are expected to respect the privacy and safety of students and staff and must comply with School requirements regarding photography, recording and distribution of images.

Security of Personal Information

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.

These steps include:

- Restricting access to information on the School databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where personal and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the School buildings and grounds to prevent break-ins.
- Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to take reasonable steps to ensure that personal information will be handled in accordance with the Australian Privacy Principles.

The School has procedures in place to identify, contain, assess and respond to suspected or actual data breaches. Where a suspected data breach is identified, the School will act promptly to contain the breach and assess whether it constitutes an eligible data breach under the Privacy Act.

Following any suspected data breach, the School will take reasonable steps to assess the potential breach and, where the breach is suspected to amount to an eligible data breach, will conduct a review of the incident to identify its cause and implement reasonable measures to prevent recurrence.

Where an eligible data breach is confirmed, the School will comply with its obligations under the Notifiable Data Breaches Scheme, including notification to affected individuals and the Office of the Australian Information Commissioner where required.

Access and Correction of Personal Information

Under the Commonwealth Privacy Act and the HRIPA, an individual has the right to seek access to, and/or correction of, any personal information which the School holds about them. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation. Access may be refused in limited circumstances prescribed by the Privacy Act or the HRIPA, including where granting access would unreasonably impact on the privacy of others or is otherwise authorised or required by law. If we decide to refuse a request for access, we will provide written notice explaining the reasons for refusal (unless it would be unreasonable to provide reasons given the grounds for refusal) and information about how to make a complaint.

Where the School corrects personal information about an individual that has previously been disclosed to a third party, the School will, upon request, take reasonable steps to notify that third party of the correction, unless doing so is impracticable or unlawful.

To make a request to access, update or correct any personal information the School holds about you or your child, please contact the School Principal by email, post or telephone at (02) 8732 7800 or email admin@mfis.nsw.edu.au.

The School may require you to verify your identity and specify what information you require. The School may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the School will advise the likely cost in advance.

The School will endeavour to respond to your access or correction request within a reasonable period of time.

Consent and Rights of Access to the Personal Information of Students

The School respects every Parent's right to make decisions concerning their child's education. Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. Generally, the School will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

Parents may seek access to personal information held by the School about them or their child by contacting the School Principal or Administration Manager by telephone or in writing (details in the section above 'Access and Correction of Personal Information'). However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the School believes the student has capacity to consent and the School is not permitted to disclose the information to the Parent without the student's consent, where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Where a student is of sufficient maturity, the School may, in appropriate circumstances, provide notices to, and seek consent from, the student directly, rather than or in addition to, their Parents, having regard to the student's individual circumstances and best interests.

Complaints

If you would like further information about how the School manages personal information, or if you would like to make a complaint regarding a breach of the Australian Privacy Principles or Health Privacy Principles, please contact the School Principal at principal@mfis.nsw.edu.au. The School's Privacy Officer is the Business Manager, unless otherwise advised by the School.

Alternatively, please contact the Principal's Personal Assistant at (02) 8732 7800 or email ea_principal@mfis.nsw.edu.au to make an appointment to discuss your matter with the Principal.

The School will acknowledge your complaint and take reasonable steps to investigate it. The School will advise you of the outcome of the investigation as soon as practicable. Where additional time is required to complete the investigation, the School will advise you accordingly.

If you are not satisfied with the School's response to your complaint, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC):

- Website: www.oaic.gov.au
- Telephone: 1300 363 992
- Post: GPO Box 5218, Sydney NSW 2001

If your complaint relates to the handling of health information under the Health Records and Information Privacy Act 2002 (NSW), you may also contact the NSW Privacy Commissioner for further information or to discuss your complaint.