Australian Islamic College Adelaide

Privacy Policy

Address: 22A Cedar Ave, West Croydon SA 5008

Tel: (08) 8340-7799 Email: info@aic.sa.edu.au Website: aic.sa.edu.au

Table of Contents

Purpose

The purpose of this Policy is to provide assistance and guidance to the Australian Islamic College (AIC) Adelaide staff, in following the new requirements that must be observed in relation to the preservation of an individual's privacy.

Your privacy is important

This statement on privacy outlines how AIC Adelaide uses and manages personal information that is provided to or collected by the College.

Australian Islamic College Adelaide is bound by the National Privacy Principles (Appendix 1) contained in the Commonwealth Privacy Act.

The type of information that the Australian Islamic College Adelaide collects and holds includes (but is not limited to) personal information, including health and other sensitive information about:

- Our students, parents and caregivers before, during and after enrolment at our College
- Job applicants, staff members, volunteers and contractors
- Other people who may come into contact with the Australian Islamic College Adelaide

Personal Information you provide

The College will generally collect personal information held about an individual by way of forms filled out by parents or students (including at enrolment), face-to-face meetings and interviews, and telephone calls. On occasion people other than parents and students may provide personal information. At the time of enrolment, parents / guardians will be supplied with a Privacy Notice (Appendix 2) outlining the College's obligations under the Privacy Act.

Personal Information provided by other people

In some circumstances the College 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 College.

Exception in relation to employee records

Under the Privacy Act, the National Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

How will the College use the personal information you provide?

The College will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Students and Parents:

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

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

- To keep parents informed of matters relating to their child's schooling, through correspondence, newsletters and magazines
- Day-to-day administration
- Looking after students' educational, social, emotional and medical wellbeing
- Seeking donations and marketing for the College
- To satisfy the College's legal obligations and allow the College to discharge its duty of care.

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

Job applicants, staff members and contractors:
In relation to personal information of job applicants, staff members and contractors, the College'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 College uses personal information of job applicants, staff members and contractors include:

- Administering the individual's employment or contract, as the case may be.
- Insurance purposes.
- Seeking funds and marketing for the College.
- Satisfying the College's legal obligations, for example, in relation to child protection legislation.

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

Marketing and fundraising:
The College treats marketing and seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to be a quality learning environment in which both students and staff thrive. Personal information held by the College may be disclosed to an organisation that assists in the College's fundraising, for example, on occasions, external fundraising organisations.

Parents, staff, contractors and other members of the wider College community may from time to time receive fundraising information. College publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Who might the College disclose personal information to?
The College may disclose personal information, including sensitive information, held about an individual to:

- Another College
- Government departments
- Medical practitioners
- People providing services to the College, including specialist visiting teachers, counsellors and sports coaches and providers of learning and assessment tools
- Assessment and educational authorities
- People providing administrative and financial services to the College
- Recipients of College publications, like newsletters and magazines
- Students, parents or guardians
- Anyone you authorise the College to disclose information to
- Anyone to whom we are required to disclose the information to by law, including child protection laws.

Sending Information Overseas

The College 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 National Privacy Principles or other applicable privacy legislation.

Electronic Storage of Information

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

An example of such a cloud service provider is Microsoft. Microsoft provides Office365 including email and document storage and also stores and processes limited personal information for this purpose. College personnel and its service providers may have the ability to access, monitor, use or disclose emails, communications (eg. instant messaging), documents and associated administrative data for the purposes of administering Office365 and ensuring its proper use.

How does the College treat sensitive information?

'Sensitive information' means information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record. This also includes personal information, health and biometric information about an 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 College's staff are required to respect the confidentiality of students’ and parents’ personal information and the privacy of individuals.

The College has in place steps to protect the personal information the College holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password protected access rights to computerised records.

Updating personal information

The College endeavours to ensure that the personal information it holds is accurate, complete and up-to-date.

A person may seek to update their personal information held by the College by contacting the Secretary of the College at any time.

Consent and rights of access to the personal information of students

The College respects every parent's right to make decisions concerning their child's education. Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The College 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 any personal information held by the College about them or their child by contacting the College Principal. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the College's duty of care to the student.

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

You May Seek Access to the Personal Information the College Holds About You

Under the Commonwealth Privacy Act an individual may seek access to personal information which the College holds about them. There are some exceptions to this set out in the applicable legislation. Students will generally have access to their personal information through their parents, but older students may seek access themselves.

To make a request to access any information the College holds about you or your child, please contact the College Principal in writing. The College may require you to verify your identity and specify what information you require. The College may charge a fee for access and will advise the likely cost in advance.

Enquiries

If you would like further information about the way the College manages the personal information it holds, please contact the Business Manager. If you believe the College has breached the Australian Privacy Principles, and wish to complain, please contact the Executive Principal. The College will investigate any such complaint and will notify you of the outcome of the investigation into your complaint as soon as it is practicable.

Procedures

1. Upon the collection of information relating to student health, office staff will file these records in student files securely in the school office.
2. Office staff cannot delegate this responsibility to others.
3. Records of behavior such as detention and suspension are filed with the relevant Coordinator. At the end of each year, these will be added into student files.
4. Information about staff details such as qualifications and tax file numbers will be filed in Payroll.
5. Sensitive information about staff in relation to grievances and misconduct will be kept in a separate locked cabinet.

Handling of suspected or known data breach

In the event of a suspected or known data breach, AIC will undertake a full and thorough investigation and in doing so will refer to the College's Privacy Breach Risk Assessment factors (Appendix 3), and will follow both the Data Breach Management Plan (Appendix 4) and the Data Breach Response Process (Appendix 5).

Reference

https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/national-privacy-principles

Implementation date:	[July 2017]
Last reviewed date:	[April 2018]
Approved by:	[Executive Principal]
Next review:	[December 2018]

Appendix 1 – National Privacy Principles

National Privacy Principles

The ten National Privacy Principles (NPPs) contained in schedule 3 of the Privacy Act 1988 regulate how large businesses, all health service providers and some small businesses and non-government organisations handle individuals' personal information.

The NPP's cover the collection, use, disclosure and storage of personal information. They also allow individuals to access that information and have it corrected if it is wrong.

NPP 1: Collection

Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.

NPP 2: Use and disclosure

Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are also rules about direct marketing.

NPP 3 & 4: Information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

NPP 5: Openness

An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.

NPP 6: Access and correction

Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: Identifiers

Generally prevents an organisation from adopting an Australian Government identifier for an individual (eg. Medicare numbers) as its own.

NPP 8: Anonymity

Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: Transborder data blows

Outlines how organisations should protect personal information that they transfer outside Australia.

NPP 10: Sensitive information

Sensitive information includes information relating to health, racial or ethnic background, or criminal records. Higher standards apply to the handling of sensitive information.

Appendix 2 – Privacy notice (provided at enrolment)

Australian Islamic College Adelaide

22A Cedar Avenue, West Croydon, SA 5008
PO Box 62, Welland SA 5007
Tel: (08) 8340 7799 Fax: (08) 8340 9988
Email: info@aic.sa.edu.au Web: www.aic.sa.edu.au

Privacy Notice

Dear Parent

Assalamua'Aleikum Wa Rahmatullahi Wabarakatuhu

Thank you for your interest in joining us at the Australian Islamic College Adelaide and choosing us to be part of your child's education.

In order to provide care, we are required to collect a range of information, some of which is defined as personal or sensitive information under the Privacy Act 1988. Under the Act, personal information manes any information or opinion about an identified, or reasonably identifiable, individual. Sensitive personal information means any information or opinion about an individual's racial or ethnic origin, political opinion or association, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, trade or professional associations and memberships, union membership, criminal record, health or genetic information and biometric information or templates.

If the relevant personal information requested in the attached enrolment documentation is not provided, we will be unable to assess your eligibility to access education and care at our service or your eligibility for any available support or funding that may be, or may become, available.

The information that you provide will only be disclosed to relevant National or State based agencies for regulatory or compliance purposes and only if that disclosure is consistent with relevant laws, in particular the Privacy Act 1988. All personal or sensitive information you entrust to us will be used, stored or disposed of, as necessary, in accordance with the Privacy Principles.

By completing and submitting the attached enrolment and associated forms, you consent to the collection of all personal information, including sensitive personal information, as contained in those forms.

Our Privacy Policy includes information about how to access, and if necessary, correct your personal information. A copy of the policy can be obtained from the school office or from our website. If you need to talk to anyone about your personal information or to make a complaint, please ask to speak to the Principal.

We would like to take this opportunity to welcome you and your family to the Australian Islamic College Adelaide.

With kind regards,

[Insert Principal's name]
Principal

Appendix 3 – Privacy Breach Risk Assessment Factors

Privacy Breach Risk Assessment Factors

Consider the type of personal information involved	
Does the type of personal information create a greater risk of harm?	Sensitive information (eg health records), or Permanent information (eg. date of birth) may pose a greater risk of harm to the affected individual/s if compromised. A combination of personal information may also pose a greater risk of harm.
Who is affected by the breach?	Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	Disclosure of a list of the names of some students who attend the College may not give rise to significant risk. Whereas, a list of students who have attended counselling support or students with disabilities may be more likely to cause harm; or Names and addresses of students or parents would have more significant risks.
Who gained unauthorised access?	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 criminal activity or a party who may wish to cause harm to the individual the information relates to. For example: If a teacher at another school gains unauthorised access to a student's name, address and grade without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.
Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not of themselves create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches are considered. This could involve incremental breaches of the same College database, or known breaches from multiple different sources (eg. multiple schools or multiple data points within the one school).
How could the personal information be used?	Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For instance, information on students domestic circumstances may be used to bully or marginalize 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?
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?
Is there evidence of intention to steal the personal information?	For instance, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in 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 behavior or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information list or stolen? Where the breach is unintentional, or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the College 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 they have, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response mush be proportionate. It is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.
Assess the risk of harm to the affected individuals	
What kind of information is involved?	Sensitive information (eg health records), or Permanent information (eg. date of birth), or a combination 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. Disclosure of a list of students who attend the College may not be sensitive information; whereas, a list of students who attend counselling support or who have disabilities may be viewed as sensitive information.
Is the information in a form that is intelligible to an ordinary person?	Examples of possible unintelligible information to an ordinary person, depending on the circumstances, may include: i. encrypted electronic information; ii. information that the College could likely use to identify an individual, but that other people likely could not (ie. student number that only the College uses (this should be contrasted with a student number that is used on public documents) iii. Information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	Encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken down 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 College 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?	Are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attach and stopped the attacker from accessing any information or copying the information?
If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?	Could an attacker have overcome network security measures protecting personal information stored on the network?
What persons, or kind of persons, have obtained or	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 criminal activity or a party who may wish to cause harm to the individual to whom the information relates.

could obtain the information?	If a teacher gains unauthorised access to a student's information without malicious intent, the risk of serious harm to the student may be unlikely.
What is the nature of the harm that could result from the breach?	Examples include, identify 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 bulling or marginalization. For example, information on students' domestic circumstances may be used to bully or marginalize the student and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may mitigate the harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorized practice, recovering records subject to unauthorized access or disclosure or loss, shutting down a system that was subject to unauthorized 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 mitigating 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 College and the particular privacy breach.
Assess the risk of harm to others	
What other possible harms could result from the breach, including harm to the College?	Examples include loss of public trust in the College, damage to reputation, loss of assets (eg stolen laptops), financial exposure (eg if bank account details are compromised), regulatory penalties (eg. for beaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

Appendix 4 – Data Breach Management Plan

Australian Islamic College Adelaide

22A Cedar Avenue, West Croydon, SA 5008
PO Box 62, Welland SA 5007
Tel: (08) 8340 7799 Fax: (08) 8340 9988
Email: info@aic.sa.edu.au Web: www.aic.sa.edu.au

DATA BREACH MANAGEMENT PLAN

	Manager of Data Breach	Person Who Identified Data Breach
Name		
Address		
Town		
State		
Post Code		
Phone		

1. Describe what the data breach was

Date data breach occurred: _____	Date data breach discovered: _____

2. What type of personal information was disclosed (please tick) -

- ☐ Financial details (eg. Credit card numbers, passwords, account information, financial statement)
- ☐ Tax File Number (TFN)
- ☐ Identity Information (eg. Centrelink Reference Number, passport number, driver license number)
- ☐ Contact Information (eg. Home / work address, phone number, email address)
- ☐ Health Information (eg. Medications, conditions, treatments)
- ☐ Other sensitive information (eg. Genetic, access or parenting plans, criminal record history)

3. Describe how the data breach occurred, who was involved and their contact details, if known

4. Identify who was responsible for the breach and their contact details

5. What is the probable intention of the person who has taken the data?

6. How many individuals' personal information was involved in the breach?

7. Describe how individuals were advised that a breach had occurred

8. Describe what remedial steps you have taken to minimise the impact of the breach on the individual

9. Have the remedial steps taken addressed the privacy breach in a timely manner? Describe how this was achieved. (If the answer is no, go to Item 10)

NOTIFY COMMISSION

10. Name who is likely to be at risk of serious harm as a result of the data breach

11. Describe the nature of the serious harm and its consequences

12. What actions are being taken to assist individuals whose personal information was involved in the breach?

13. List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to

14. List identifiable actions that can be taken to minimise recurrence of the subject data breach

Appendix 5 – Data Breach Response Process