Iona College

Privacy Policy

CONTENTS

1 RATIONALE

Iona College (the College) is a Catholic Boys School conducted by the Oblates of Mary Immaculate. The College caters for over 1500 students ranging from year 5 to year 12.

The purpose of this privacy policy is to:

- Describe the types of personal information that the College collects, holds, uses and discloses
- Outline the College's personal information handling systems and practices
- Enhance the transparency of the management of the College's personal information
- Explain our authority to collect your personal information, why it may be held and how it will be used and protected
- Notify if the College is likely to disclose your personal information; if so to whom and when
- Provide information on how you can access your personal information, correct it if necessary and engage a complaints process if you believe it has been wrongly collected or inappropriately handled.

The College, including its employees, contractors and agents is subject to the *Privacy Act 1988* (the Privacy Act) and is bound by the requirements under the Australian Privacy Principles (APPs) contained in the Privacy Act.

The policy covers how the College will collect and handle personal information, including sensitive information.

2 GLOSSARY

Personal information refers to information (or an opinion), whether true or not, in any form that can identify a living person.

Sensitive information refers to personal information that is of a sensitive nature, including information about health, genetics, biometrics or disability; racial or ethnic origin; religious, political or philosophical beliefs; professional association or trade union memberships, sexuality or criminal record.

The Australian Privacy Principles (APPs) are contained in schedule 1 of the *Privacy Act 1988* outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

Primary Purpose refers to the particular purpose for which information is collected.

Secondary Purpose is any purpose other than the primary purpose for which the APP entity collected the personal information.

3 INFORMATION HANDLING PRACTICES

Iona College will generally collect information held about an individual by way of forms filled out by parents or pupils, face-to-face meetings, interviews, emails and telephone calls. On occasions people other than parents and pupils provide personal information.

Information may be collected directly from you or from a representative that has been authorised to provide such information.

As outlined under the APPs, the College will only collect information for a lawful purpose that is reasonably necessary or directly related to one or more of our functions and activities.

The College collects and holds a broad range of personal information which relates to:

3.1 Personal Information

Personal information may be collected directly by the College or by organisations acting on the College's behalf (for example, contracted service providers such as medics for AIC sport). All contractors and subcontractors of the College are required to comply with the same privacy requirements applicable to the College.

3.2 Sensitive Information

Sensitive information may be collected under the obligations imposed by the APPs. Sensitive information may only be collected when:

- consent has been provided
- it is authorised by law
- a permitted general situation exits such as to prevent a serious threat to safety.

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 disallowed by law.

3.3 Students and parents and/or guardians before enrolment, during the course of enrolment and after graduation, including:

- Name, contact details (including next of kin), date of birth, previous school and religion
- Medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors
- 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
- Any court order
- Volunteering information
- Photos and videos at school events
- Other information that is relevant to the schooling process

3.4 Job applicants, staff members, volunteers and contactors, including:

- Name, contact details (including next of kin), date or birth and religion
- Information on job application

- Professional development history
- Salary and payment information, including superannuation details
- Medical information (e.g. details of disability and/or allergies, and medical certificates
- Complaint records and investigation reports
- Leave details
- Photos and videos taken at school events
- Workplace surveillance information
- Work emails and private emails when using work email address and internet browsing history
- Other information that is relevant to the employment process

The College also holds information about 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.

3.5 Exception in relation to employee records

Under the Privacy Act 1988, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to Iona College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between Iona College and employee.

4 THE PRIMARY USE OF INFORMATION COLLECTED FROM 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 quality education to the student, exercise its duty of care and perform necessary associated administrative activities, which will enable the students to take part in all the activities of the school. This includes satisfying the needs of parents, the needs of the student and the needs of the College throughout the whole period the student is enrolled at the College.

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

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

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

4.1 Collecting personal information from children and young people

In carrying out the College's functions and activities information may be collected about children and young people, either directly from them or through their parents or guardians. Where children are over the age of 16 the College may collect information directly from them as they are more than likely to have the capacity to understand any privacy notices provided to them and to give informed consent to collection. For children under the age of 16 or where capacity to provide consent is an issue the College's policy is that a parent or guardian will be notified and their consent sought.

5 THE PRIMARY USE OF INFORMATION COLLECTED FROM JOB APPLICANTS, STAFF MEMBERS AND CONTRACTORS

In relation to the personal information of job applicants, staff members and contractors, the College's primary purpose of collection is to assess and (if successful) engage the applicant, staff member or contractor as the case may be. Personal information is then used for the primary purpose of:

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

6 THE PRIMARY USE OF INFORMATION COLLECTED FROM VOLUNTEERS

The College obtains personal information about volunteers who assist the College in its functions or activities. In relation to the personal information about volunteers, the College's primary purpose of collection is to assess and (if successful) engage the volunteer as the case may be. Personal information is then used for the primary purpose of:

- Administering the volunteers contact, engagement with the College as the case may be
- For insurance purposes, and
- Satisfying the College's legal obligations, for example, in relation to child protection legislation

7 SECONDARY USES OF INFORMATION COLLECTED

Personal information will only be used for secondary purposes where it can be done so in accordance with the *Privacy Act 1988*. This may include where you have consented to this secondary purpose, or where the secondary purpose is related to the primary purpose and you would reasonably expect us to use or disclose the information for the secondary purpose, where it is required or authorised by law or a situation exists to prevent a serious threat to safety or similar.

7.1 Marketing and fundraising

Marketing and donations for the future growth and development of the school as an important part of ensuring that the College continues to be a quality learning environment in which students and staff thrive. Non-sensitive personal information held by the College may be disclosed to an organisation that assists the College in fundraising; for example the College's foundation or alumni organisation, church and parish authorities.

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 which may be used for marketing purposes.

8 COLLECTION OF UNSOLICITED INFORMATION

Sometimes information is not sought by us but is delivered or sent to us by an individual or third party without prior request. Where unsolicited information is received by us, we will, within a reasonable period, determine if that information is directly related to one or more of our functions or activities. If the information is not relevant, the College will as soon as practicable destroy the information. If the use of this information is related to the primary function of the College the information will be treated in line with the APP's and this policy.

9 REMAINING ANONYMOUS OR USING A PSEUDONYM

In some cases an individual may wish to remain anonymous or use a pseudonym when dealing with the College; this may be an important element of privacy when interacting with our organisation. In circumstances where it is likely the College would need to collect your personal information, such as to resolve a dispute or provide you with a service, the College will notify the individual accordingly at the time of collecting the information.

10 STORAGE AND DATA SECURITY

The College holds personal information in a range of paper-based and electronic records, including offsite storage. The College takes all reasonable steps to protect the personal information held against loss, unauthorised access, use, modification, disclosure or misuse. Access to your personal information held is restricted to authorised persons who are College employees or contractors, on a need to know basis.

11 DISCLOSURE OF PERSONAL INFORMATION

Iona College may disclose personal information, including sensitive information, held about an individual to:

- another school;
- government departments;
- medical practitioners;
- people providing services to Iona College, including specialist visiting teachers, counsellors and sports coaches;
- recipients of College publications, such as newsletters and magazines;
- parents;
- anyone you authorise Iona College to disclose information to;
- anyone to whom we are required to disclose the information to by law; and
- other people and/or organisations on a need to know basis where their involvement is needed for the College to perform its primary function

Information collected by the College will only be disclosed for the same purpose that it was collected or at times a directly related secondary purpose.

Information provided to other authorities will be under that organisation's privacy policy. Information provided within the College organisation to contractors, volunteers and employees will be bound by the College's Privacy Policy.

11.1 Sending and storing information overseas

The College may disclose personal information about an individual to overseas recipients, in the following situations:

- The publication on the internet of material which may contain personal information, such as photographs, video recordings and audio recordings; and posts comments on our social media platforms;
- The provision of personal information to overseas researchers or consultants (where consent has been given for this or we are otherwise legally able to provide this information);
- The provision of personal information to recipients using a web-based email account where data is stored on an overseas server; and
- The provision of personal information to foreign governments and law enforcement agencies (in limited circumstances and where authorised by law).

However, Iona College will not send personal information about an individual outside Australia without:

- The recipient being subject to a law or binding scheme substantially similar to the Australian Privacy Principles, including mechanisms for enforcement;
- Disclosure is required by law;
- Disclosure is reasonably necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body and the recipient performs similar functions.
- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

Iona College may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as services relating to email, 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 that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

An example of such a cloud service provider is Microsoft. Microsoft provides the Office 365 Suite including Exchange Online, and stores and processes limited personal information for this purpose. School personnel and their service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering Office 365 and ensuring its proper use.

12 IONA COLLEGE WEBSITES AND PORTALS

When using online College services such as websites and portals hosted in the iona.qld.edu.au domain, servers automatically record information that your browser sends whenever you visit. These server logs may include information such as your IP address, your top level domain name, the date and time of the visit to the site, the pages accessed and the documents viewed, previous sites visited, the

browser type, the browser language, and one or more 'cookies' that may uniquely identify your browser.

No attempt is made to identify you through your browsing other than in exceptional circumstances such as investigation into improper use of a service.

12.1 Website analytics

To improve your experience on our site, we may use 'cookies'. Cookies are an industry standard and most major web sites use them. A cookie is a small text file that our site may place on your computer as a tool to remember your preferences. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of our websites.

The College uses Google Analytics, a service which transmits website traffic data to Google servers in the United States. Google Analytics does not identify individual users or associate your IP address with any other data held by Google. We use reports provided by Google Analytics to help us understand website traffic and webpage usage.

Users consent to the processing of data about you by Google in the manner described in Google's Privacy Policy - external site and for the purposes set out above. You can opt out of Google Analytics if you disable or refuse the cookie, disable JavaScript, or use the opt-out service provided by Google - external site.

12.2 Links to external websites

College websites include links to other websites. We are not responsible for the content and privacy practices of other websites. We recommend that you examine each website's privacy policy separately.

12.3 Electronic communication

There are inherent risks associated with the transmission of information over the internet, particularly via email. You should be aware of this when sending personal information to us via email or via our website or social media platforms

13 ACCESS AND CORRECTION OF PERSONAL INFORMATION

All reasonable steps are taken to ensure that the personal information that is collected is accurate, up to date, complete, relevant and not misleading. These steps include responding to requests to correct personal information when it is reasonable and appropriate to do so.

Under the Commonwealth Privacy Act [and the Health Records Act], an individual has the right to obtain access to any personal information which Iona College holds about them and to advise Iona College of any perceived inaccuracy. Pupils will generally be able to access and update their personal information through their parents.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information Iona College holds about you or your child, the College should be contacted in writing. Iona College may require you to verify your identity and specify what information you require. Iona College may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the

information sought is extensive, Iona College will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

14 CONSENT AND RIGHTS OF ACCESS TO THE PERSONAL INFORMATION OF PUPILS

Iona College respects every parent's right to make decisions concerning their child's education. Generally, Iona College will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's parents. Iona College will treat consent given by parents as consent given on behalf of the pupil, and notice to parents will act as notice given to the pupil.

In cases where the release of information may have an unreasonable impact on the privacy of others or where the release of information may result in a breach of the College's duty of care, the College may require a formal application through the Right to Information (2009). After this application the College reserves the right to apply for an exemption under the Act.

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

15 DATA BREACH RESPONSE PLAN

A data breach is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference, for example:

- A device containing personal information is lost or stolen
- The College's information system or an associated database is hacked
- Personal information is mistakenly provided to the wrong person.

The first 24 hours after discovering a data breach are crucial to the success of the response. A quick response can substantially decrease the impact on the affected individuals. A data breach response plan is a framework which outlines the roles and responsibilities for managing an appropriate response to a data breach. The aim of this data breach response plan is to:

- Meet obligations under the Privacy Act
- Protect the personal information of staff, students, volunteers and parents
- Deal with adverse media or stakeholder attention from a breach or suspected breach
- Instill public confidence in the College's capacity to protect personal information by properly responding to the breach.

15.1 Data Breach Response Team

The Data Breach Response Team consists of the Privacy Officer (Dean of Analytics and Performance), Principal, ICT Manager, Human Resources Manager and the Risk and Compliance Officer.

15.2 Actions Required for Data Breach Response

Staff who become aware of a Privacy Breach must immediately notify the Privacy Officer or a member of the Iona Leadership Team who will notify the Data Breach Response Team.

The notification should include:

- Time and date of suspected breach.
- Personnel involved.
- The cause and extent of breach.
- Who may be affected.

15.2.1 Contain the breach and evaluate the risks.

- Establish who is affected by the breach/
- Are multiple individuals affected by the breach?
- What personal information is involved in the breach?
- Identify the date, time, duration and location of the breach?
- Is there (now or in future) a real risk of serious harm to the affected individuals
- Does the breach or suspected breach indicate a systemic problem with practices and procedures
- Does there need to be a public notification in relation to the breach?
- What is the risk of harm to the College and the individuals affected?
- What is the likely recurrence?
- What is the likely cause of the breach?
- Other issues relevant to circumstances
- Notification to the Rector

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

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Privacy Breach, but there is an indication of a systematic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

15.2.2 Notification

The main consideration before choosing what action to take is to ask: "Is there a real risk of serious harm to affected individuals or the College?

The Data Breach Response Team will determine whether to affected individuals, parents, the Privacy Commissioner and/or other stakeholders.

If communication is deemed necessary a communication strategy should be developed which outlines:

- Who is responsible for implementing the communication strategy
- Determining how affected individuals will be contacted
- Criteria for determining which external stakeholders should be contacted (e.g. law enforcement, cyber security agencies, regulators including the OAIC and the media)

- Who is responsible for determining which external stakeholder is to be contacted
- Who is responsible for liaising with those stakeholders

15.2.3 Prevent further breaches

The Privacy Breach must be fully investigated by the College and the breach and its cause must be recorded on the Privacy Breach Log.

The Privacy Officer must conduct a post-breach review to assess the effectiveness of the College's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Plan.

The Privacy Officer must, if necessary, make appropriate change to policies, procedures and training practices including updating this Privacy Breach Response Plan.

The Privacy Breach Log will be reviewed annually by the College Leadership Team.

16 ENQUIRIES AND COMPLAINTS

If you would like further information about the way Iona College manages the personal information it holds, or wish to complain that you believe that Iona College has breached the Australian Privacy Principles please contact the Iona College Privacy Officer who will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.