



# Privacy Policy

<b>Document name:</b>	Privacy Policy
<b>Applies to:</b>	Whole College
<b>Contact person:</b>	College Principal
<b>Date last reviewed:</b>	October 2025

## Purpose and scope

Masada College protects personal information in accordance with the Privacy Act 1988 Commonwealth and the Australian Privacy Principles. For health information we also comply with the Health Records and Information Privacy Act 2002 NSW. This policy explains what we collect, why we collect it, how we use and disclose it, how we secure and retain it and the choices and rights available to you.

Employee records exemption

Some handling of current or former employee records that is directly related to the employment relationship is exempt under the Privacy Act. We still treat staff information with care and in line with this policy where practicable.

## Who this policy covers

- Students and their parents or carers
- Staff contractors volunteers and job applicants
- Visitors to our campus and website
- Any individual who interacts with the College

## What we collect

We collect only what is reasonably necessary for our functions and activities.

- Identity and contact details including name date of birth address contact details and emergency contacts
- Student records including enrolment attendance academic progress behaviour and wellbeing notes learning support assessments and reports
- Health information including medical conditions allergies disabilities immunisation records care plans and counselling notes where relevant to our duty of care

- Family and legal information including parenting orders or court orders relevant to student welfare and authorised pick ups
- Financial information including billing and payments
- Employment information for staff and contractors including Working With Children Check qualifications references onboarding payroll and superannuation performance and leave records noting the employee records exemption
- Images and surveillance including photographs and video from College activities. Closed Circuit Television operates on campus for safety and security and may be used to review serious behaviour issues as they arise. Community Security Group has access to College CCTV for security purposes and may monitor the campus and immediate surrounds to help protect people and property in line with our agreement and applicable law
- Information technology and systems including limited logs from College systems and networks as described in College use policies
- Website analytics our website may collect limited analytics information using cookies. You can adjust your browser settings to refuse cookies

## How we collect information

- Directly from you including forms interviews meetings phone and email and College systems or portals
- From third parties where lawful and appropriate including previous schools health practitioners government education or assessment bodies referees and service providers that support our information technology and learning platforms
- Through systems and security including learning platforms CCTV and staff email and internet logs in accordance with notified policies

## Why we collect and use information

- Provide education and student support including teaching learning support co curricular wellbeing excursions and duty of care
- Operate the College including enrolment administration communications with families timetabling fees and payments fundraising and alumni relations. You can opt out of marketing by contacting us
- Legal and compliance including child protection critical incident management reportable conduct work health and safety government reporting audits and responses to lawful requests
- Security including preventing detecting and responding to risks threats and incidents on or around our campus which may involve the use of CCTV and cooperation with Community Security Group and law enforcement
- Child safety information sharing. We may share information with prescribed bodies to support the safety welfare or wellbeing of a child or young person in line with Chapter 16A of the Children and Young Persons Care and Protection Act 1998 NSW
- Staff and contractor management including recruitment onboarding payroll performance professional learning and safety

**We only use or disclose information for the purpose we collected it for a related purpose that individuals would reasonably expect with consent or as required or authorised by law.**

# Disclosures including to service providers

We may disclose information to:

- Education partners and authorities including previous or next schools and assessment or support specialists
- Health and wellbeing providers including doctors psychologists and allied health where needed for student care
- Government and oversight bodies where required
- Government and sector reporting including data required for national or state education reporting such as ACARA student background characteristics and other mandatory collections
- CRICOS and ESOS compliance. Where relevant to international students we disclose information necessary to meet obligations under the Education Services for Overseas Students Act and the National Code
- Service providers including information technology platforms cloud storage communications finance and audit legal and insurance transport and approved photographers
- Community Security Group for campus and community security activities including access to and use of CCTV
- Law enforcement emergency services and regulators when necessary for safety and security or as required by law
- Others as authorised or requested by you or as required by law

## Overseas disclosures and cloud services

Some trusted providers may store data outside Australia for example mainstream cloud and education platforms. When we disclose information overseas we take reasonable steps to ensure recipients protect it consistently with the Australian Privacy Principles including contractual safeguards, access controls and vendor due diligence. Contact the Privacy Contact if you have questions about specific vendors.

## Direct marketing

We follow Australian Privacy Principle 7 and the Spam Act. For electronic marketing we use consent and provide a simple way to stop future messages by contacting the College. Requests to stop will be actioned within a reasonable time.

## Data security

We use appropriate technical and organisational measures to protect information from misuse interference loss and unauthorised access modification or disclosure. These include role based access strong authentication secure storage for paper records staff training vendor and access reviews and secure destruction methods.

## **Data retention**

We retain records for as long as required for our functions by law or for prudent record keeping. For example key academic records may be retained long-term, most financial and staff records at least seven years and child protection and serious incident records as required by law. We may securely destroy or de-identify information when it is no longer needed.

## **Notifiable data breaches**

If a data breach is likely to result in serious harm we will promptly assess the incident and where an eligible data breach is identified we will notify affected individuals and the Office of the Australian Information Commissioner and include steps individuals can take to protect themselves. We maintain a data breach response plan and a record of assessments and notifications.

## **Student privacy and mature students**

We usually engage with parents or carers for students under 18. Considering age, maturity and circumstances we may engage directly with a student about their information particularly for sensitive health matters where appropriate and consistent with our duty of care and applicable laws.

## **Workplace surveillance NSW**

For staff and certain contractors we may use cameras computer and information technology and email and internet monitoring in accordance with the Workplace Surveillance Act 2005 NSW. We provide advance written notice and maintain clear policies. Blocking of emails or sites occurs only in line with a notified policy and where required we issue prevented delivery notices.

## **Access and correction**

You may request access to or correction of your personal information. We will respond within a reasonable time generally within thirty days and may need to verify identity. We may refuse access in limited circumstances permitted by law for example safety risks or privacy of others. If we refuse we will tell you why and how to complain. We do not charge for correction requests and will advise of any reasonable access fees in advance.

## **Complaints**

If you are concerned about how we handle personal information please contact us first so we can try to resolve the issue. If you remain unsatisfied you may complain to the Office of the Australian Information

Commissioner or to the NSW Information and Privacy Commission for health information matters under the HRIP Act.

## **Contact us**

Privacy Contact Head of Business Operations

Masada College St Ives NSW 2075

Phone 02 9449 3744

## **Changes to this policy**

We may update this policy to reflect legal or practice changes. The current version is on our website. Significant changes will be communicated through College channels.