Metavision Institute Pty Ltd
A.C.N 102 838 844

Privacy Policy

Purpose

This policy sets out how Metavision Institute collects, uses and processes personal data, as well as ensuring that information about staff members, contractors, suppliers, students, clients, alumni and other stakeholders is kept confidential. Information collected by or provided to Metavision Institute will be used only in the ways described in this policy, and in accordance with Metavision Institute's obligations as a higher education provider in regard to the collection, storage and use of information.

The following Acts and the Privacy Management Framework set out the principles and processes that Metavision Institute must abide by when it collects, stores, uses and discloses Personal Information: The Information Privacy Act 2002, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and the Office of the Australian Information Commissioner's Privacy Management Framework.

Scope

This policy applies to all members of Metavision Institute's community.

Relevant TEQSA Threshold Standards

This policy aligns with

Related HESF Domain	Section	Standard
Domain 2: Learning Environment	2.3, 2.4	Wellbeing and Safety; Student Grievances and Complaints
Domain 6: Governance and Accountability	6.2	Corporate Monitoring and Accountability
Domain 7:	7.2, 7.3	Information for Prospective and Current Students; Information Management

1 Policy

1.1. Metavision Institute collects personal information from a variety of sources about staff, prospective and enrolled students, alumni, governance committee members and stakeholders. Information may be collected from a range of sources, including the following:

1.1.1. Course application form, assignment extension request form, critical incident report, formal complaint and appeal applications,

1.1.2. Prospective students entering personal information into the online application form,

1.1.3. Course Download Form, Enquiries Form, Contact form on Metavision Institute's website,

1.1.4. Email, telephone or mail,

1.1.5. Engagement via social media on Metavision Institute's Facebook page, Instagram and LinkedIn,

1.1.6. Participation in any course, workshop, activity, or event offered by Metavision Institute

1.1.7. Industry partners and host organisations providing work integrated learning experiences,

1.1.8. Staff performance reviews, supervisory meetings and leave applications,

1.1.9. Applications and interviews for employment, contract work or as a supplier to Metavision Institute,

1.1.10. Personal information from education agents in relation to prospective overseas students, which is collected to facilitate the application and enrolment process,

1.1.11. When required to do so by law (for education, child protection, occupational health and safety or other legislation in Australia), and

1.1.12. Assignments submitted through the Learning Management System Sophia and client information presented in supervision by students to meet the requirements of their enrolled course.

1.1.13. Tutorial recordings made via Zoom for units in which a student is enrolled, which are transferred to and stored on Metavision Institute's Google Drive. Recordings may capture the voice, image, and personal contributions of participants.

1.2. The information that Metavision Institute may collect about students, staff, contractors, suppliers, alumni, governance committee members and stakeholders includes:

1.2.1. Names,

1.2.2. Dates of birth,

1.2.3. Contact information, including email addresses, home addresses, phone numbers, Skype addresses,

1.2.4. Demographic information such as postcodes, age, and gender,

1.2.5. Licence number, passport number, bank account details, ACN, ABN, and Tax File Number,

1.2.6. Unique Student Identifier (USI),

1.2.7. Information about employment background, work experience, and references,

1.2.8. Information about circumstances affecting study such as disabilities and special circumstances, and

1.2.9. Financial information and banking details

1.3. Metavision Institute collects and uses personal information for the following purposes:

1.3.1. To verify identity,

1.3.2. To access and update student records in the USI Registry System and to report student outcomes,

1.3.3. To respond to queries relating to courses, units, workshops, requests for academic advice, complaints and services,

1.3.4. To better understand student needs, and enable Metavision Institute to improve its courses, services and the student experience on the basis of formal feedback,

1.3.5. To provide marketing information about courses, professional development seminars and services to students, and to request relevant information to manage and administer courses and services, including prior qualifications, enrolment, assessment, and issuing of testamurs, records of results and statements of results,

1.3.6. For internal records,

1.3.7. For assessment in Metavision Institute’s higher education and other courses,

1.3.8. To report on student outcomes according to requirements of the Tertiary Education Quality Standards Agency (TEQSA),

1.3.9. To report to TEQSA and the Department of Education on key personnel and fit and proper persons responsible for the management of Metavision Institute, and

1.3.10. To employ and manage staff, contractors and suppliers.

1.4. Modes of communication

1.4.1. Metavision Institute communicates with staff, contractors, suppliers, prospective and enrolled students, alumni, governance committee members and stakeholders by telephone, email, SMS, social media, the website, and/or mail. Staff, contractors, suppliers, enrolled students, and governance committee members are expected to maintain up to date contact details.

1.4.2. Information transmitted over the internet cannot be guaranteed to be secure. Metavision Institute cannot guarantee the security of any electronic information that is transmitted or received.

2 Disclosure of stored Personal Information

Metavision Institute will provide access to personal information it holds:

2.1 If Metavision Institute obtains written permission from the relevant party to provide access to the information;

2.2 Under relevant legislation, and depending on circumstances:

2.2.1 Department of Education,

2.2.2 TEQSA,

2.2.3 Australian Tax Office,

2.2.4 Social Research Centre (QILT surveys),

2.2.5 Education agents (with student's consent),

2.2.6 Superannuation funds, and

2.2.7 Centrelink

2.3 Metavision Institute may disclose personal information in order to:

2.3.1 Assist with core functions such as the recruitment of students and provision of IT services,

2.3.2 Verify educational information details upon request from third parties, such as verifying completed courses and qualifications, and articulation into other higher education courses offered by external institutions,

2.3.3 Comply with Metavision Institute's legal and regulatory obligations, including disclosure and reporting to Commonwealth, State and Territory government agencies for planning, evaluative, administrative and funding purposes. This may include:

2.3.3.1 Disclosure and reporting to Commonwealth and State government agencies for the purpose of administrating entitlements to financial assistance under Commonwealth programs for supporting students, such as FEE-HELP, and

2.3.3.2 Disclosure and reporting to TEQSA

2.3.4 Notify credit reporting agencies and courts, tribunals, and regulatory authorities where students fail to pay for goods or services provided by Metavision Institute to them, when internal avenues for remedy have been exhausted,

2.3.5 Respond to courts, tribunals, regulatory authorities, and law enforcement officers as required by law in connection with any actual or prospective legal proceedings, or in

order to establish, exercise or defend Metavision Institute's legal rights,

2.3.6 Communicate with relevant third party or parties, with relevant consent, if a matter involves third parties. When Metavision Institute discloses personal information to third parties, it will request or otherwise seek confirmation that the third party follows Australian Law and Privacy Principles regarding management of personal information,

2.3.7 Pay wages, superannuation and other relevant employment benefits, and contractor and supplier entitlements, and

2.3.8 Protect the safety of students, staff, students' clients, contractors and suppliers in the case of risk of safety.

3 Data security

3.1 Metavision Institute is committed to ensuring that the information provided by staff, students, alumni, committee members and stakeholders is stored securely. In order to prevent unauthorised access or disclosure, Metavision Institute has appropriate physical, electronic and administrative processes in place to safeguard and secure information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

3.2 Metavision Institute takes seriously the risk of a breach of data security and takes reasonable steps to reduce the risk of a breach. Data security is included in Metavision Institute's Risk Management Framework.

3.3 The Executive Committee monitors risk to data security. The Chief Executive Officer will immediately report a notified breach of data security to the Governance Board, including a plan for how to reduce risk of harm to affected individuals (for example, change of password if an email or student account has been subject to unauthorised access).

3.4 The Chief Executive Officer will report Notifiable Data Breaches to affected individuals and the Privacy Commissioner (for example, if stored information on Tax File Numbers has been accessed) when serious harm is likely and remedial action taken by Metavision Institute has not reduced the risk of harm.

3.5 Metavision Institute uses cookies on its website. Cookies are small files sent from the web server to users' web browsers which do not contain personal information. Cookies allow access and navigation, analyse web traffic and remember users' choices. Cookies do not give Metavision Institute access to users' computers or information, other than data provided by users. Users can choose to accept or decline cookies.

3.6 Metavision Institute's website may provide links to other websites of interest. Metavision Institute does not have control over other websites. Prospective and current students are to exercise caution when accessing such websites.

3.7 Tutorial recordings are collected for the purpose of providing enrolled students with access to unit content. Recordings are stored in Zoom Cloud on collection and are subsequently transferred to Metavision Institute's Google Drive. Access is restricted to the tutor, students enrolled in the relevant unit, and authorised staff including IT administrators. Student access to tutorial recordings is available for one year from the end of the unit in which the recording was made. Metavision Institute retains tutorial recordings for two years from the end of the unit for quality assurance and assessment review purposes, after which recordings are deleted. During the second year of retention, access is restricted to authorised MI staff only. In accordance with Australian Privacy Principle 11.2, recordings are not retained beyond two years from the end of the unit. The IT Manager is responsible for implementing a deletion schedule consistent with this clause.

4 Control of Personal Information

4.1 Choice and Consent

4.1.1 In order for Metavision Institute to fulfil its duties as a provider of accredited higher

education courses and services, enrolled students, staff, contractors and suppliers are required to disclose certain personal information.

4.1.2 Personal information is protected by this policy. Metavision Institute will not sell, distribute or release personal information to third parties unless it has permission or is legally required to do so.

4.2 Restrict collection or access

4.2.1 Students, alumni, staff, contractors, suppliers and stakeholders may choose to restrict the collection or use of personal information.

4.2.2 Students who have previously agreed to Metavision Institute using their personal information for marketing purposes may change their mind at any time by notifying the Student Liaison Officer.

4.3 Access to personal information

4.3.1 Students, alumni, staff, contractors, suppliers and stakeholders may request access to personal information held by Metavision Institute in accordance with the provisions of the Privacy Act.

4.3.2 A small administrative fee may be payable for the provision of personal information. Metavision Institute will require evidence of identification prior to releasing information and reserves the right to refuse to provide individuals with such information in certain circumstances as set out in the Act.

4.4 Correction of personal information

4.4.1 If students, alumni, staff, contractors, suppliers or stakeholders believe that personal information stored by Metavision Institute is inaccurate, out of date, incomplete, irrelevant or misleading, a request for the information to be rectified or updated is to be submitted to the Chief Executive Officer.

4.4.2 Metavision Institute relies in part upon individuals advising any changes in their personal information.

4.4.3 Metavision Institute will promptly respond to requests to correct personal information within a timeframe of up to five working days.

4.5 Students, alumni and stakeholders may unsubscribe from the email database, or opt out of communications, by emailing the Administrative Officer.

5 Complaints

5.1 If students, alumni, staff, contractors, suppliers or stakeholders believe that Metavision Institute has breached its privacy obligations or this policy, the relevant policy is to be followed in raising a grievance or making a complaint: the Staff Grievance and Complaints Policy or Student Grievance, Complaints and Appeals Policy (Non-Academic).

5.2 Complaints will be responded to within the framework of the relevant policy.

5.3 To contact Metavision Institute about privacy concerns, email the Chief Executive Officer.

6 Responsibilities

6.1 Governance Board

6.1.1 Approves, provides oversight and reviews this policy

6.1.2 Monitors the implementation of this policy and ensuring there is a system in place to report data breaches

6.2 Chief Executive Officer

6.2.1 Implements policy and reporting to Governance Board

6.3 Line managers

6.3.1 Train new staff in privacy obligations and management in the Induction period

6.4 All staff members, contractors and suppliers

6.4.1 Meet obligation to protect such information in accordance with the relevant legislation and this policy

6.4.2 Report unauthorised access to their email accounts or to documents stored electronically, or any other data breach to the Chief Executive Officer

6.5 Students

6.5.1 Report unauthorised access to the Administration Office

6.6 Affected users

6.6.1 Change passwords online immediately following the receipt of a report of unauthorised access and assess whether any other action is required

6.7 Executive Committee

6.7.1 Monitor and report on Metavision Institute's privacy management and any breach of this policy, and planning for prevention

Definitions

Term	Definition
Personal Information	Any information that allows individuals to be identified, including any information relating to a person's study or work at Metavision Institute as an employee, contractor or supplier. Metavision Institute considers any information that an individual discloses in public online forums or other interactive media to be public information which therefore may not be protected.
Data Breach	An unauthorised access or disclosure of personal information, or loss of personal information. A data breach may result from malicious action, human error or a data systems failure
Notifiable Data Breach	Data breach involving personal information that are likely to result in serious harm to any individual affected, and requires specific steps to be taken. The Notifiable Data Breach scheme was established by the passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017.

Related Documents

Category	Documents
Policies	Assessment and Moderation Policy
	Critical Incident Policy
	Course Evaluation and Review Policy
	Information Management and Security Policy
	Records Management Policy
	Staff Grievance and Complaints Policy
	Staff Performance Review and Management Policy
	Staff Selection, Recruitment, Appointment and Professional Equivalency Policy

	Student Grievance, Complaints and Appeals Policy (Academic)
	Student Grievance, Complaints and Appeals Policy (Non-Academic)
	Student Information and Communication Policy
	Student Recruitment, Admission and Enrolment Policy
Other	Business Continuity Plan
	Risk Management Framework
	Risk Register
	Student Handbook
	Assignment Extension Request Form
	Course Application Form
	Critical Incident Report Form
	Formal Complaints and Appeals Lodgement Form

Version Control

Field	Detail
Document Title	Privacy Policy
Approved by	Governance Board
Version No.	V1.3, Reviewed August 2026
Date approved	8 September 2026
Replaces Version No.	V1.2
Next review due	3 years after approval
Custodian	Dean