



Melbourne Metrics

Privacy and security guidelines for partners

Melbourne Metrics at the University of Melbourne provides assessment, reporting and credentialing services for schools and education providers via the University's Ruby platform. This document outlines the privacy and security capabilities and infrastructure provided by the University of Melbourne and specific arrangements in place for the Ruby platform.

Privacy at the University of Melbourne

The University's [Privacy Policy \(MPF1104\)](#) affirms the University's commitment to the privacy and data protection principles contained in relevant privacy laws. This policy applies to all areas of the University. Any person who deals with the University is entitled to expect that their personal and health information will be treated in accordance with this policy.

The University has obligations under the Privacy and Data Protection Act 2014 (Victoria) and to the extent that they apply to our activities the Privacy Act 1988 (Commonwealth of Australia) and the European Union General Data Protection Regulation 2016/679 (which relates to the personal information of individuals located in the European Economic Area).

Security at the University of Melbourne

The University of Melbourne takes a risk-based approach to cybersecurity under the authority of the Chief Technology Officer and the Director of Cybersecurity. The University works to continuously evolve its cybersecurity capabilities to prevent, detect, disrupt and respond to existing and emerging cyberthreats. A range of administrative, technical and physical procedures have been designed to protect the information stored in the University environment. As part of this approach, the University embeds security considerations into the design and architecture of information technology systems and business processes. The Cyber Security team is engaged for all key projects to ensure a forward-thinking approach to security.

The University maintains an Information Security Policy (MPF1270) and Provision and Acceptable Use of IT Policy (MPF1314) as part of the Melbourne Policy Framework to govern security for teaching and learning, corporate enterprise use, contracted service providers, contracted/funded research and collaborations, sensitive and classified information and international travel. These are reviewed on an ongoing basis to enable the University to respond to emerging threats or identified control deficiencies. The University aligns itself where possible to international standards such as ISO27001 and the NIST Cybersecurity Framework.

Overview of the Ruby platform

The Ruby Platform (Ruby) is a cloud based, multi-tenant suite of technologies designed and validated over a 10-year period at the University of Melbourne to support Melbourne Metrics' partners to scale the use of next-generation assessment and reporting methods that recognise and celebrate learner attainment in transferrable learning competencies. The Ruby platform is fully owned by the University of Melbourne.

Ruby is designed for modern learning communities:

- Secure, cloud-based, Software as a Service (SaaS) offering.
- Easy-to-use interfaces for system leaders, school leaders, teachers, assessors, and students.
- Flexible enough to fit a wide range of curricula, learning designs and school programs across early childhood education to senior secondary and beyond.
- Built to assess and report on any framework of transferable learning competencies adopted by a school or system, including competencies such as, for example, agency in learning, collaboration, communication, entrepreneurship, active citizenship, personal enterprise, quality thinking, self-motivated learning, principled action, and collective engagement.

Ruby is a full-service enterprise platform supporting all aspects of the assessment and recognition process within and across schools, including:

- Delivery of assessment tools.
- Secure data collection and storage of assessment information.
- Support for process control in and across schools that reflect various assessment designs (who assesses whom and when).
- Provision of various forms and formats of reporting of learner attainment.
- Support for quality monitoring (reliability, validity, calibration of standards, fairness, comparability and moderation).
- Management of certification and credentialing processes and associated storage and dissemination methods.

It offers schools and education systems a platform that combines technical quality and assessment rigour and capacity to configure to a system's policies and each school's particular implementation.

Integrations

Ruby currently supports several levels of integrations with School Information Systems (SIS) and credentialing/recognition platforms. Ruby currently allows for SIS integration via Wonde, www.wonde.com, and is integrated with the Universities Admissions Centre's CredNet platform (www.crednet.com.au) to issue and store verified credentials. Melbourne Metrics considers integration with other platforms on a case-by-case basis, and if:

1. The integration aligns with Ruby's specific needs and is complementary to, or extends functionality
2. It meets our partner's objectives and enhances their experience
3. Technical, privacy and cybersecurity standards are met
4. Adequate funding is secured to cover development, implementation, and ongoing maintenance costs.

Privacy Impact Assessments and privacy collection notices

The University conducts a Privacy Impact Assessment (PIA) for each major initiative supported by Ruby, at least once every five years for standard use of the platform, and whenever significant changes are made to the system or its data processing activities, ensuring ongoing compliance with data protection regulations and safeguarding the privacy rights of individuals. PIA's involve analysis of all data flows, processing and analysis of data, data quality and management and transborder data flows. A privacy collection notice (PCN) for Ruby is available within each instance of the platform, and separately on request. The privacy collection notice (PCN) supports the principle of responsible and transparent handling of personal information by explaining generally what information the University collects and why, who we share it with, and how individuals can exercise their rights regarding their information. The PCN requires consent from users prior to use of the platform.

Server and instance arrangements

Separate servers and instances of Ruby are configured in Australia, Singapore and the United States, utilising Amazon Web Services (AWS) as the cloud infrastructure provider.

Australia and United States server:

Each configuration is completely independent. The Australian configuration is deployed in the Sydney and Melbourne regions. The USA configuration is deployed in the Virginia region. All data, including backups, are resident in their own region or country.

Singapore server:

The Singapore configuration is used for processing and storage of operational data independently, with data backups stored in the Sydney and Melbourne regions of Australia.

Security processes and arrangements

The University's platform includes the following security protections:

- Complete authentication and authorisation mechanisms, following best practice in security.
- Evidence and inputted data is timestamped and not modifiable.
- Restricted user access
 - Restricted user access based on roles. Each individual has their own dedicated access account. Access is granted through a levelled structure: System administrators grant access to project administrators; project administrators grant access to school administrators; and school administrators grant access to teachers at their school.
 - Higher privileged accounts have more protection mechanisms. Two-factor authentication is enforced for all system, project and school administrators. Protected access to infrastructure via multifactor authentication and IP address restriction.
 - System administrators' computers are further protected by data encryption. Data is downloaded and de-identified for system administrators when troubleshooting is required. Access is temporarily disabled for system administrators when going for extended periods of leave.
 - No unauthorised access or modification.
- Executed agreements and contracts including relevant terms and conditions.
- A security schedule is in place which includes regular penetration testing. The latest test was conducted in 2025.

Contact and other information

Melbourne Metrics welcomes questions and discussion on privacy and security matters, please contact:

melbassess-info@unimelb.edu.au

Frequently asked questions

Is there an Information Security Policy and how is compliance ensured?

The University of Melbourne has an [Information Security Policy](#) and all employees including contractors undergo regular mandatory training to ensure compliance.

What identity and access management controls are employed?

The University follows an access control management process which manages the user identity lifecycle as well as access to information assets and enterprise systems based on the principles of 'Least Privilege' and 'Need to Know'. The Ruby platform implements various role types with permissions assigned to role types, not directly to users. Users are assigned to the appropriate role based on their access needs and responsibilities and inherit the permissions assigned to the role. Multiple methods including lock out, time out, multifactor authentication, and IP address restrictions are used depending upon account sensitivity and configurations.

What technical data management controls are employed?

Data is encrypted both during transfer and storage using industry-standard methods. Backups are automated across different accounts and regions. We regularly check that backups are intact. Operational and archive backups have separate access controls, with archive data restricted to backup administrators. We don't use real data for testing; when necessary, we remove all personal information from production data before using it in test environments, such as for troubleshooting.

What network and hosting infrastructure controls are employed?

The network is divided into public, private, and internal sections for security. Strict rules control network traffic, specifying exact ports and servers. Web Application Firewalls protect all public access points and act as a Network Intrusion Detection System. All servers have anti-malware, file integrity checks, and intrusion prevention. We regularly scan for vulnerabilities and apply patches. Development, testing, and production environments are kept completely separate.

What types of personal data is required for the use of Ruby?

The amount and type of personal data required varies depending on your specific instance of the platform and the required configuration for assessment, reporting, and credentialling. We advise you to consult your instance directly for details. As a general principle, we collect only the minimum personal data necessary to operate the platform and assessment, reporting, and credentialling service effectively.

Is data used for research purposes?

Data use for research purposes is determined by the terms outlined in the agreement with your school, network or department. You can also consult the privacy collection notice within your particular instance of the platform.

What data retention policies are in place?

For details on data retention, please refer to the [University's Records Management Policy](#).

Where is customer data stored?

For International Big Picture Learning Credential activities in the USA, customer data is hosted in AWS data centres located in Virginia, USA.

For international school activities as part of the New Metrics International School Program, Singapore AWS data centres are used for processing and storage of operational data, with backups stored in AWS data centres located in Sydney and Melbourne.

For other programs and activities, customer data is hosted in Australia, specifically in AWS data centres located in Sydney and Melbourne.

Who owns the data stored or created using the service?

Data ownership is determined by the terms outlined in the agreement with your school, network or department.

Is any customer data sold to third parties?

No, Melbourne Metrics at the University of Melbourne does not sell any customer data.

Is customer data shared with any third parties?

Please consult the privacy collection notice within your particular instance of the platform. This notice is customised to reflect the privacy considerations relevant to the assessment, reporting, and credentialing configuration of that instance.

In general, customer data is shared with:

- contracted service providers or partners engaged by us to perform legitimate functions on our behalf
- contractors engaged by the University of Melbourne to manage the technical deployment and support of the Ruby platform;
- your school, education institution, government department or organisation that has engaged the University of Melbourne to fulfil our obligations in delivering our services.

Do customers have control over their stored data?

Yes, customers may request access to or correction of their personal information in accordance with the [University of Melbourne's Privacy Policy](#).

How is client data secured and transferred securely?

Client data is encrypted at rest and stored on secure networks. AES-256 encryption is used for all data at rest and for backups. Data is encrypted during transit using the latest TLS protocols.

How often are security tests such as penetration testing conducted?

Penetration testing is performed by third-party security testing companies every 12 to 18 months or when significant security configuration changes occur. Internal vulnerability scans are conducted every day.

What happens in the event of a service outage?

In the case of a service interruption, Melbourne Metrics will make best attempts to inform system users through platform notices.

Does the service support multifactor authentication (MFA)?

For operational simplicity, MFA is generally not implemented for school-based staff members to streamline workflow and reduce potential access barriers, however, it can be configured on request.

MFA is mandatory for all system administrators, regardless of their level. It is also required for any access to Amazon Web Services (AWS). Additionally, remote access to the University network is only possible through a Virtual Private Network (VPN) connection that also employs MFA.

What international standards is the service aligned with?

The University of Melbourne's Information Security Policies and related procedures align with ISO 27001 and the University maintains an ISO 27001 certification for specific IT environments. The Ruby application is not hosted within this environment and has not been assessed by an independent auditor. However, it is governed by the same Information Security Policy. Melbourne Metrics is committed to continuously identifying and managing risks and maturing the solution's compliance to the policy.

Does the University act as a data importer under the European Union's General Data Protection Regulation (GDPR)?

Yes, the University has a separate agreement for schools in the European Union. Please refer to the terms outlined in the agreement with your school, network or department regarding the GDPR.

Does the University act as an Overseas Recipient under China's Personal Information Protection Law (PIPL)?

Yes, the University has a separate agreement for schools in the People's Republic of China (PRC). The University will provide a pre-filled Standard Contract for Outbound Cross-border Transfer of Personal Data to facilitate the transfer of personal information in accordance with PIPL. Schools must complete remaining details and then the Standard Contract can be signed by both parties. Schools then need to complete a filing of documents to the Cyberspace Administration of China (CAC). A sample student/guardian consent form prepared in accordance with PIPL requirements can also be shared with schools to assist with consent processes if requested.

Is there a Risk Management Framework in place?

Yes, the University follows a Risk Management Framework aligned with AS/NZS ISO 31000:2018.

What child protection measures are in place?

The University has a Child Safety Policy (MPF 1337) which aligns with the Victorian Child Safe Standards made under the Child Wellbeing and Safety Act 2015 (Vic). The Standards are set of mandatory requirements to protect children and young people from harm and abuse and apply to all Victorian organisations that work or volunteer with children. All University staff are required to complete Child Safety Training on a regular basis and are required to obtain and maintain an employee Working with Children Check. Additional screening is conducted for certain projects and engagements, on request.

Are regular internal or external reviews performed?

Various central services at the University of Melbourne, including Enterprise Services, Legal Services, and Privacy and Records, conduct internal reviews, endorsements, or approvals. These processes cover multiple aspects such as architecture design, privacy, cybersecurity, legal considerations, and data and records management. It's important to note that each department has a different level of authority, and their reviews may not be equivalent to a formal audit.

External reviews are conducted on infrastructure, directly by the cloud hosting provider. It covers architecture, security, operation, reliability, and performance.

How does the organisation protect against cyberattacks?

A multi-layered defence strategy is employed, including risk assessments, training, network security, and data encryption.

Do systems have real-time antivirus scanning?

Yes, real-time scanning is enabled, and antivirus definitions are updated hourly.

How are real or potential security incidents managed?

The University of Melbourne has an [Information Security Policy](#) that requires all systems and services to have a plan for managing security incidents, like data breaches or cyberattacks.

Has the service experienced any security incidents in the past year?

No security incidents have been reported in the past 12 months.

What Disaster Recovery (DR) process is in place?

Disaster recovery is built into the system. Backups are automated across different accounts and regions, limiting potential data loss to 5 minutes at most. Recovery time ranges from 4 hours for a server failure to 3 days if an entire AWS region goes down. We test our full disaster recovery plan yearly, making sure we can restore the entire system from scratch if needed.

What is the financial viability of the organisation running the service?

Annual operational and financial reports for the University of Melbourne are available via: [University of Melbourne Annual Reports](#).

Will Single Sign-On be supported?

Single Sign-On will be supported from 2026, including Open ID Connect and SAML 2.0.

What customer support is available?

Helpdesk support is provided between 9am and 4:30 pm (EST) Monday to Friday, excluding public and university holidays. The level of helpdesk support provided, whether first-level (direct to schools) or second-level (through an appointed network or department coordinator), is determined by the specific agreements in place with each school, network or department.