Moodle data privacy:

Trust by design

moodle™

Table of contents

Executive summary

Data privacy is no longer just a legal requirement—it's a core expectation from learners, educators, and institutions worldwide. As scrutiny of digital platforms grows, Moodle stands apart with a commitment to transparency, control, and user protection that's built into every layer of our ecosystem.

This whitepaper explores how Moodle approaches data privacy across **Moodle LMS**, **Moodle Workplace**, and the **Moodle App**—highlighting the role of Moodle Certified Partners in delivering trusted, privacy-first learning environments. Unlike commercial platforms that monetise user data or limit control, Moodle empowers organisations to manage data on their terms, supported by a global community, privacy-focused tools, and flexible hosting options.

You'll find:

- A clear overview of Moodle's privacy principles and design choices
- Comparisons to mainstream platforms and common pitfalls in the sector
- Practical privacy measures every institution can adopt
- Insights into regulatory compliance and ethical learning environments

Moodle is more than a learning management system—it's a privacy-respecting alternative in a world that too often overlooks privacy. And this document is both a guide and a call to action: for learning technologists, institutions, and partners to centre data protection in their practice, and to choose tools that put people first.

Why data privacy matters

From universities to government agencies to global enterprises, organisations today are entrusted with growing volumes of personal data. Whether it's a learner's course progress, an employee's performance review, or a citizen's certification record, the expectation is clear: data should be protected, handled responsibly, and never exploited.

But this expectation often clashes with reality. Around the world, digital platforms have come under fire for opaque data practices, invasive tracking, and limited user control. In some cases, tools designed for convenience or scale have compromised the very trust that learning environments rely on.

The privacy reckoning in EdTech and workplace tools

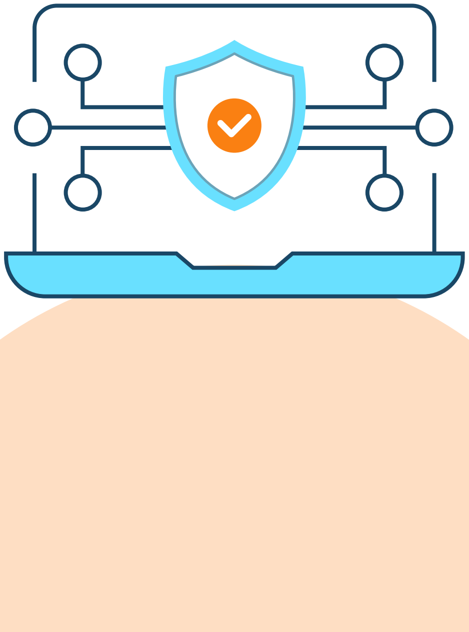
The shift to digital learning—accelerated by global events such as the COVID-19 pandemic—has amplified awareness of data rights. High-profile investigations into EdTech vendors have revealed how some platforms collect and monetise data beyond their educational or training purpose, often without meaningful consent. For workplace training, compliance tools, and learning apps, concerns about third-party tracking and cross-purpose data use are just as real.

At Moodle, we believe in a different approach—one that's grounded in privacy by design and driven by mission, not monetisation. As a **Certified B Corporation** with a global reach, we focus on building tools that support ethical, user-controlled learning environments.

Security by design

Moodle follows a "**security and privacy by design**" approach to development, aligned with global standards such as the **OWASP Top Ten** and **CIS Controls**. We run a global **Vulnerability Disclosure Programme** through **Bugcrowd** and ensure every new feature is reviewed for potential risks before release.

For a full overview of how we embed security across our platform, see the **Moodle security: Building trust through open collaboration whitepaper**.



Privacy is foundational to learning and trust

Protecting privacy isn't just about regulation—it's about trust. For a learner to engage fully, or an employee to grow confidently, or a citizen to participate in a training program, they must trust that their data is safe, private, and used only for its intended purpose.

Data privacy builds:

- **Confidence** in the learning environment
- **Compliance** with global regulations like **GDPR**, **FERPA**, **POPIA**, and **HIPAA**
- **Control** for organisations to govern their own systems and data flows

Whether you're delivering accredited degrees, onboarding new staff, or managing large-scale skills programs, the integrity of your platform—and the choices it makes around data—has never mattered more.

Privacy by design: How Moodle embeds data protection into its DNA

While often used interchangeably, **privacy** and **security** are distinct—but closely connected—concepts. Security is about protecting data from unauthorised access, breaches, or misuse. Privacy, on the other hand, is about ensuring that an individual's data is collected, used, and shared in ways they understand and agree to.

A platform can be secure without being privacy-respecting—but not the other way around. That's why Moodle takes a holistic approach: combining robust security architecture with deep respect for user privacy. From Moodle LMS to Moodle Workplace and the Moodle App, our products are built to give organisations control, ensure compliance, and uphold the rights of every user.

Transparent and user-controlled

Moodle is built to give organisations—not vendors—control over how data is stored, managed, and accessed.Whether hosted on-premises or with a **Moodle Certified Partner**, site administrators have visibility into:

- Who can access data
- What data is collected
- Where data is stored
- How long it is retained

Tools for publishing policies, managing user consent, and reviewing data requests are built into the platform, empowering compliance with local regulations like GDPR, POPIA, and FERPA.

Designed for diverse environments

Moodle supports a range of deployment needs—from secure offline government networks to cloud-hosted public networks—while maintaining consistent privacy protections across all environments. Role-based access, encryption protocols, and user-level consent features enable governments, universities, and businesses alike to tailor their installations while adhering to common privacy standards.

This flexibility ensures that Moodle can operate in complex, multi-stakeholder environments without compromising on data protection. And because our products are modular and open, privacy features can be extended, adapted, or integrated with internal compliance workflows.

Control, choice, and compliance

Data privacy isn't just about what a platform does with your data—it's about what it allows you to do with it. At Moodle, we believe organisations should have full control over how data is collected, managed, stored, and erased. Our role is to provide the tools, flexibility, and transparency needed to support that control—no matter where or how a Moodle platform is deployed.

Full ownership and autonomy

Unlike many proprietary platforms, Moodle doesn't lock you into one way of working. Whether you're running a corporate training programme, a national education portal, or a university-wide virtual learning environment, you remain the data controller. Moodle gives you:

- **Freedom to choose** where and how your data is hosted
- **Granular control** over data access and retention
- **Tools to publish, track, and enforce data policies**
- **Built-in support for user consent and legal age verification**

This level of autonomy is especially valuable in regulated environments—where compliance with laws like GDPR, FERPA, POPIA, or HIPAA is essential, and where control over data flows is a matter of legal and organisational risk.

Embedded tools for compliance

Moodle includes a suite of features designed to help organisations meet their privacy obligations and demonstrate compliance:

- Policy manager: Publish mandatory and optional policies that users must agree to before accessing the platform.
- Age verification: Enforce minimum age requirements based on your jurisdiction.
- Data requests: Enable users to request a copy of their data or ask for its deletion.
- Data registry: Maintain a centralised overview of all personal data types stored in your Moodle site, their purpose, and retention period.
- Privacy officer role: Assign responsibility for overseeing privacy management within your site.

These tools are available in Moodle LMS and Moodle Workplace—with additional administrative permissions and multi-tenant controls available in Workplace for managing compliance across departments, agencies, or client groups.

Compliance without compromise

Some platforms claim to support compliance, but offer little visibility into where data is stored or what third parties can access it. Moodle takes the opposite approach. By giving you choice of infrastructure, transparent documentation, and access to the underlying system, we help you implement privacy practices that align with your organisation's policies—not just our own.

When working with a **Moodle Certified Partner**, you may benefit from enhanced compliance services such as audit-ready hosting, regular patching, and data handling aligned to international standards. However, practices can vary by provider.

We recommend asking specific questions to understand how your hosting partner—or any vendor—addresses key privacy concerns:

How is personal data stored, protected, and backed up?

What privacy and security certifications or audits are in place?

How are software updates and security patches managed?

Where is data physically hosted, and does it align with your regional requirements?

These questions can help ensure your hosting setup supports your organisation's data protection obligations.

Moodle vs the market: Privacy that puts people first

In an era of data exploitation and opaque platform practices, Moodle stands apart. While other learning platforms are being scrutinised for intrusive data collection, surveillance-based business models, or limited transparency, Moodle takes a different route—one grounded in respect, not revenue.

We do not sell user data. We do not run ads. We do not track users across the web.

Instead, we prioritise user control, institutional ownership, and long-term trust.

A growing trust gap in digital learning

Recent investigations have highlighted how many EdTech and corporate learning platforms gather far more data than needed—often without users' full knowledge. Some platforms rely on behavioural tracking, share data with advertisers, or offer limited opt-out mechanisms. Even when tools are free or subsidised, users may be paying with their data.

Government agencies, universities, and businesses are rightly pushing back—demanding platforms that respect the principles of consent, purpose limitation, and data minimisation.

Moodle's privacy promise

Moodle offers a credible alternative:

- **Open, inspectable code:** Anyone can verify how data is processed—no black boxes.
- **User-centred design:** Features like policy management, data request tools, and role-based permissions are built-in.
- **Ethical foundations:** As a purpose-driven organisation and certified B Corporation, our incentives are aligned with the public good—not investor returns.
- **Modular architecture:** You decide which plugins, integrations, and data pathways are used—not us.

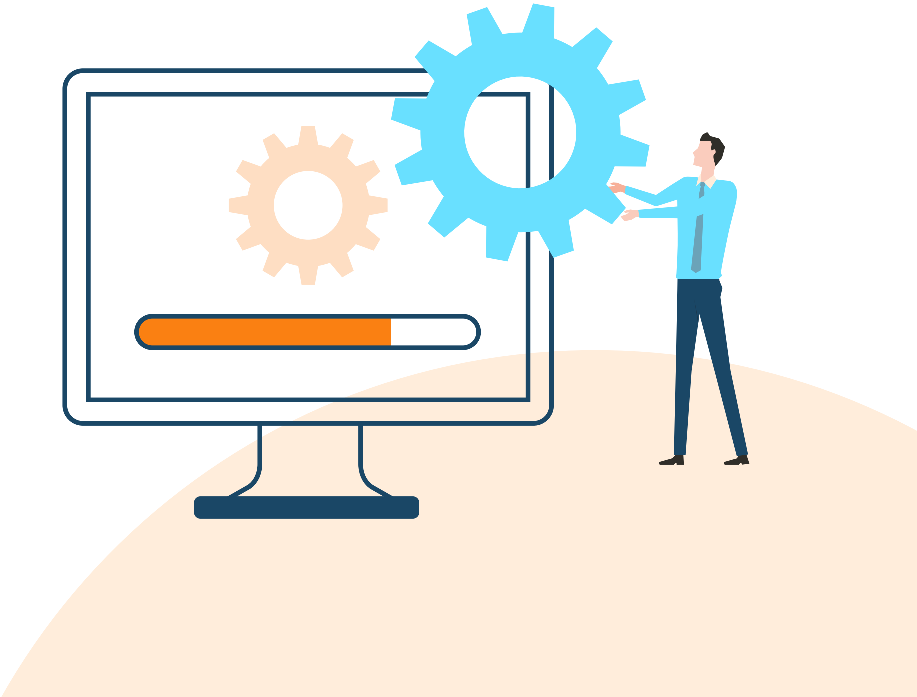
Moodle's privacy-first approach is especially valued by:

- Government organisations, seeking sovereign control and alignment with national data strategies
- Higher education institutions, subject to student protection laws and academic integrity standards
- Corporations and non-profits, managing employee data and compliance across global regions

Not just compliant—transparent

Unlike some providers who treat compliance as a checkbox, Moodle believes privacy should be understandable and explainable. Our **documentation** is public. Our **development** process is open. And our tools are designed to give organisations the clarity they need to meet both legal and ethical obligations.

Where others obscure, Moodle opens. Where others restrict, Moodle enables. In a crowded market of platforms making privacy promises, Moodle delivers on them—by design.



Hosting and accountability: Why the right partner matters

A secure, privacy-respecting platform isn't just about the software—it's about how and where it's hosted. Even the most well-designed tools can become vulnerable if deployed without proper controls, monitoring, or governance. At Moodle, we treat hosting not just as an infrastructure decision, but as a critical layer of privacy protection.

Control over your data, from the ground up

Moodle gives organisations the freedom to choose a hosting setup that aligns with their privacy requirements, risk appetite, and internal capabilities. You can **download Moodle** and self-host or work with a **Moodle Certified Partner**—offering scalable, secure, and compliant solutions tailored to your needs.

No matter the model, one principle remains: **you retain ownership of your data.**

- You decide where data is stored and who can access it
- You control retention policies, backups, and recovery
- You choose the level of external support that fits your needs

The role of Moodle Certified Partners

For organisations with high compliance obligations—such as government bodies, multinational companies, or universities processing sensitive learner data—working with a Moodle Certified Partner can offer peace of mind and enhanced accountability.

Certified Partners provide hosting environments specifically optimised for Moodle. To ensure your provider meets your privacy and compliance needs, ask whether they offer:

- **GDPR-aligned data handling practices**
- **Regular software and security updates**
- **Encryption at rest and in transit**
- **Audit-ready logging and backup systems**
- **Support for complex deployments or multi-tenancy structures**

These questions can help you evaluate whether your hosting partner is equipped to support secure, privacy-first learning at scale.

Certified Partners can also help with vendor risk assessments, regional data residency requirements, and internal privacy audits—making them a strategic choice for long-term sustainability and compliance.

The risks of opaque or unmanaged hosting

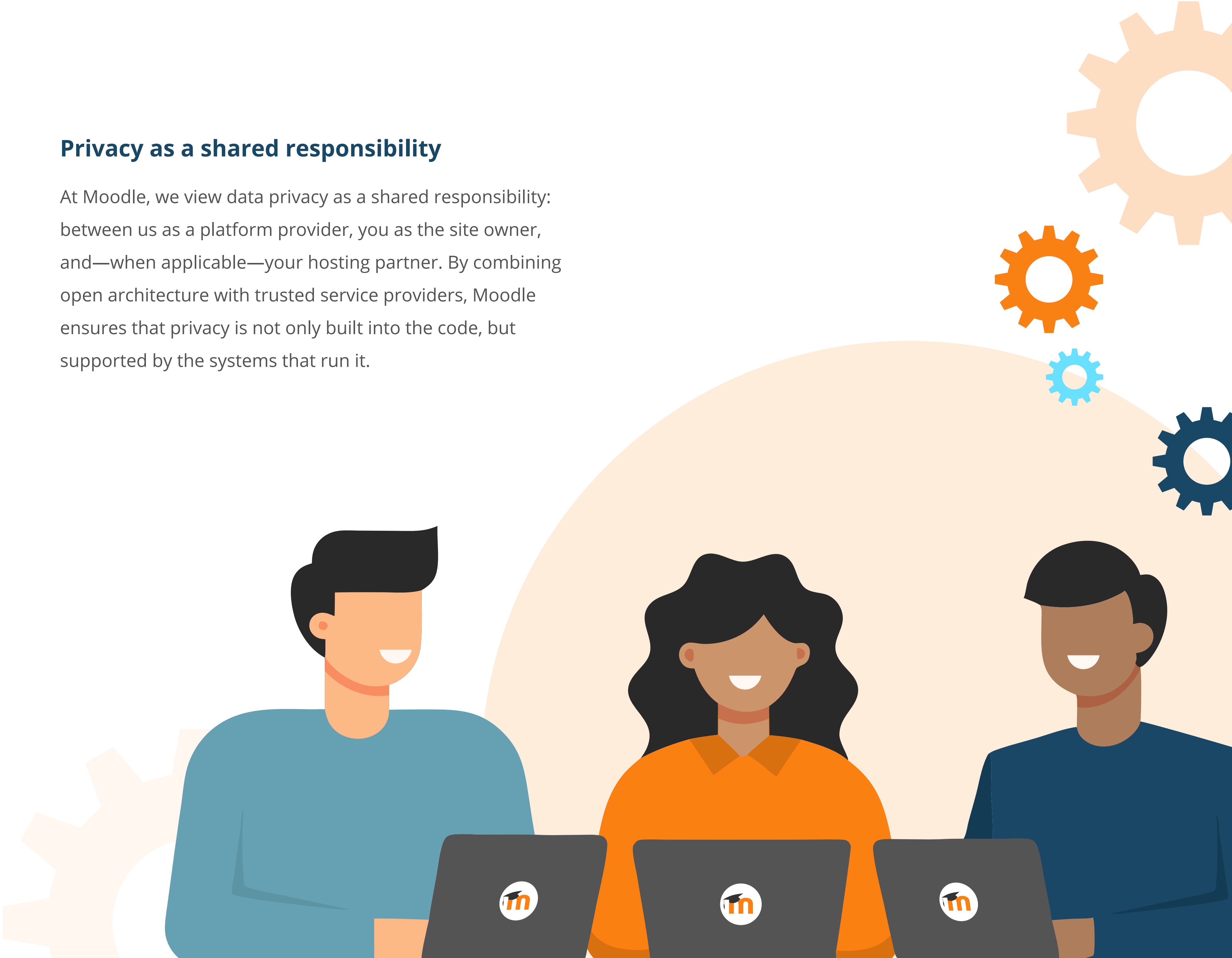
By contrast, platforms that limit access to back-end settings, offer no visibility into data flows, or delay critical patches introduce real risk. Poorly managed environments can lead to:

- Data breaches from unpatched software
- Accidental exposure due to misconfigured permissions
- Inability to comply with access, export, or deletion requests
- Regulatory penalties from non-compliance

Privacy is not just a feature—it's a practice. And that practice must extend to the infrastructure your platform relies on.

Privacy as a shared responsibility

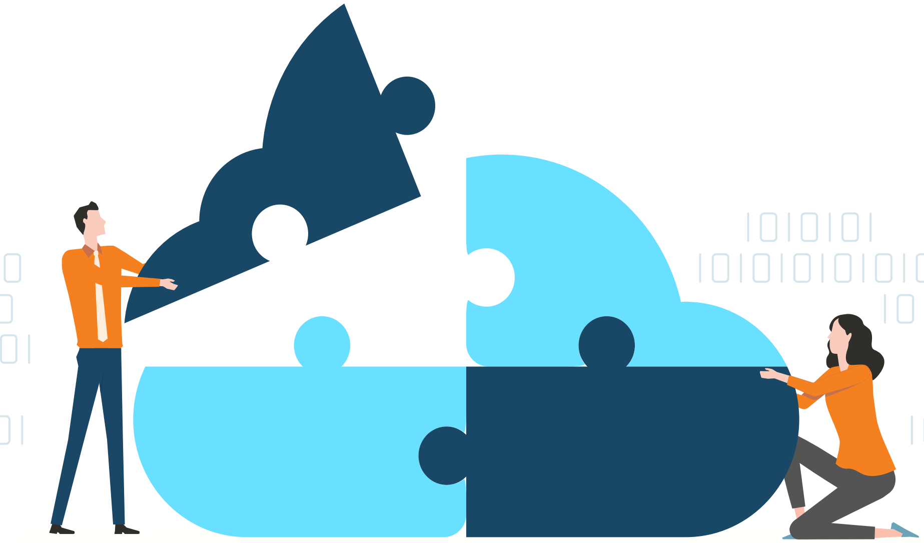
At Moodle, we view data privacy as a shared responsibility: between us as a platform provider, you as the site owner, and—when applicable—your hosting partner. By combining open architecture with trusted service providers, Moodle ensures that privacy is not only built into the code, but supported by the systems that run it.



Practical privacy:
What every Moodle site should be doing

While Moodle provides the tools, features, and architecture to support data privacy, compliance ultimately rests with the organisation using the platform. Whether you're running a government training portal, a corporate onboarding programme, or a large university LMS, proactive privacy management is essential.

This section outlines recommended practices for Moodle site administrators to strengthen privacy protections and meet local legal obligations.



1. Publish and manage your site's privacy policies

Use Moodle's **Policy handler** to create, display, and track agreement to policies such as:

- Site privacy notice
- Cookies or analytics disclosure
- Terms of service or acceptable use
- Age of consent (where applicable)

Policies can be mandatory or optional and linked to specific user roles or activities.

2. Assign a Privacy officer

Designate a staff member or team to take ownership of data privacy governance within your site. Moodle includes a **Privacy officer role** with special capabilities to:

- View and manage user data requests
- Approve or deny data deletions and exports
- Oversee retention rules in the data registry

This ensures there's clear accountability and oversight for all privacy-related actions.

3. Enable and respond to user data requests

Moodle supports the full lifecycle of **subject access and erasure requests**, including:

- Requesting to download personal data
- Requesting deletion of data (subject to retention rules)
- Viewing request status within a user's profile

These features help you fulfil obligations under laws such as GDPR, FERPA, or other regional data protection frameworks.

4. Use the Data registry to define retention rules

The Data registry allows you to document:

- What types of personal data are stored
- Why each data type is collected
- The legal basis for processing
- Retention periods and auto-deletion options

This registry provides a clear record for internal governance and external audits.

5. Enforce age-based access where needed

If your site serves young learners, Moodle can enforce digital age of consent thresholds and capture parental consent where required—helping you comply with regulations like COPPA or similar regional laws.

6. Use roles and permissions to limit data access

Limit access to personal data using Moodle's granular roles and permissions system. For example, training supervisors in a business context should only access their direct team's progress—not data across the organisation.

7. Review your site's security settings

Strong privacy relies on strong security. Regularly review the Security overview report and ensure that:

- HTTPS is enforced across all pages
- Default roles have only necessary permissions
- Session handling and password policies are up to date

8. Partner with experts if you need help

For organisations with limited internal resources, partnering with a Moodle Certified Partner can help ensure that best practices are applied and maintained over time.

This checklist is not exhaustive—but it's a starting point. Implementing even a few of these practices can significantly reduce risk, improve user trust, and streamline compliance.

9. Enable encrypted push notifications in the Moodle App

When using the Moodle App, enable support for end-to-end encrypted push notifications to protect user messages in transit. This optional feature adds an extra layer of privacy, ensuring that sensitive information—such as assignment reminders or grade alerts—is transmitted securely, even across mobile networks. Read more about Moodle App security.

Product spotlight: Privacy-first platforms for enterprise, education, and public sector

While Moodle's core privacy philosophy applies across all products, each platform offers specific features and configurations tailored to different use cases. Here's how data privacy is approached in Moodle Workplace and the Moodle App.

Moodle Workplace: Privacy at scale

Moodle Workplace extends Moodle LMS with enterprise-grade features, including multi-tenancy, advanced reporting, and automation. It's designed for organisations delivering structured training at scale—internally or externally.

At its core, Moodle Workplace uses a shared database structure, but privacy boundaries between tenants are strictly enforced. By default, no personal data is shared across tenants, and users remain unaware of other tenants' existence—ensuring GDPR-aligned separation of data by default and by design. Administrators can configure visibility settings for specific use cases, but cross-tenant sharing must be explicitly enabled.

Key privacy features include:

- **Data segmentation and role scoping:** Each tenant operates as an independent data environment, with separate configurations for permissions, roles, and reports.
- **Customisable data retention and consent rules:** Define how long data is stored and how consent is gathered, by tenant or audience.
- **Support for decentralised access control:** Assign local administrators within tenants while maintaining global oversight.
- **Designed for regulated and high-compliance environments** across government, corporate, and public sectors.

Where certain jurisdictions or institutional policies require physical separation of data between entities, Moodle recommends deploying separate Moodle instances rather than relying on logical separation alone. This flexibility ensures compliance without compromising privacy or performance.

When paired with a Moodle Premium Certified Partner, Moodle Workplace becomes a powerful foundation for scalable, audit-ready learning systems with privacy protections built in.

Moodle App: Mobile privacy by design

The Moodle App brings the learning experience to mobile devices—without compromising privacy.

- **No tracking or data collection by the Moodle App** when connected to your site
- **All communications occur directly between user and site**, not third parties
- **Optional encrypted push notifications**, managed by the institution: When enabled, push notifications are end-to-end encrypted during transit, giving organisations added control over how mobile data is handled
- **Minimum-permissions model:** App only requests access to device features when needed
- **Supports age verification and policy display** on first launch

Designed to extend—not expose—your Moodle site, the app gives users flexibility and institutions full control over data behaviour on mobile.

Looking ahead:
A global perspective on learning and data rights

The right to privacy is more than a policy checkbox—it's a cornerstone of dignity, autonomy, and trust in the digital age. Around the world, lawmakers, institutions, and citizens are rethinking how data is collected, used, and protected. This shift is especially critical in learning environments, where data often reflects not only what people know, but who they are.

At Moodle, we believe that education technology must uphold the highest standards of privacy. Not only because it's required by law—but because it's the right thing to do.

Aligning with global rights frameworks

Moodle's open architecture and user-first philosophy align naturally with international frameworks like:

- **GDPR (EU):** Emphasising data minimisation, transparency, and individual rights
- **FERPA (US):** Protecting the confidentiality of learner education records
- **POPIA (South Africa) and LGPD (Brazil):** Driving localised privacy accountability
- **The UN Convention on the Rights of the Child:** Asserting children's rights to digital privacy and protection

By building tools that empower rather than extract, Moodle helps organisations across sectors uphold these frameworks—while adapting to local needs and regulations.

From compliance to ethical leadership

As pressure grows on platforms to do better, Moodle's model—rooted in openness, autonomy, and ethical service—provides a path forward. Our community isn't just responding to compliance requirements. It's leading conversations about **ethical data stewardship** in education, workforce development, and public training.

Across higher education, business, and government, Moodle sites are showing that it is possible to build learning ecosystems that are powerful, scalable, and privacy-respecting—without compromising on usability, performance, or trust.

Our commitment

We'll continue to evolve our products with privacy in mind, to support localised needs while upholding global values. We'll advocate for greater transparency and control across the learning technology landscape. And we'll keep working with our community, partners, and customers to ensure that the future of learning is not only effective—but respectful, responsible, and fair.

Because data privacy isn't just a feature.
It's a foundation.

moodle™

Ready to take the next step?

Whether you're looking to strengthen compliance, improve data governance, or implement privacy best practices, a Moodle Certified Partner can help.

Get expert support tailored to your organisation's needs—so you can deliver trusted, privacy-first learning experiences with confidence.

Get in touch today