toddle

Privacy & Security Pack

How Toddle protects your data

Last Updated: March 12, 2025

This pack describes the current state of Toddle's security, which is subject to change with future enhancements and product launches. This document is for informational purposes only and does not constitute legal advice, nor should it be interpreted as supplementing or being incorporated into any terms and conditions of any contractual agreements.

Table of contents

One of our core values is to grow responsibly. It is **our commitment to uphold the trust** that you have placed in us by sharing your data.

Deepanshu Arora
CEO, Toddle

Introduction

Toddle is entrusted with safeguarding the valuable teaching and learning data of over 2,000 schools worldwide. This commitment to data protection is demonstrated through an annual SOC 2 Type II audit, which verifies adherence to stringent standards for security, availability, and confidentiality. Toddle also holds ISO certifications, including ISO 27001, the internationally accepted standard for Information Security Management Systems (ISMS), underscoring its dedication to comprehensive data security.

In this pack, Toddle outlines the measures, practices, and technologies that form the foundation of its security strategy, ensuring it remains a trusted partner for educators and schools globally.

Useful Links

Cookie Policy | Toddle

Terms of Service | Toddle

Terms of Use | Toddle

Third-Party Service Providers | Toddle

Children's Online Privacy Protection Act (COPPA) | Toddle

Family Educational Rights and Privacy Act (FERPA) | Toddle

GDPR | Toddle

CCPA | Toddle

DPDPA | Toddle

KSA PDPL | Toddle

HK PDPO | Toddle

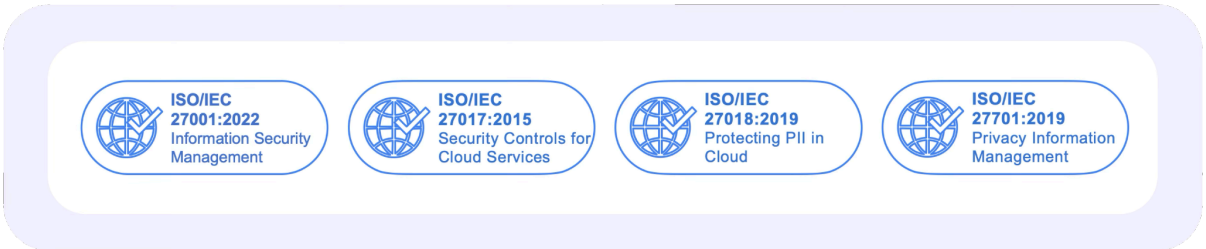
Australian Privacy Principles | Toddle

Trust Vault | Toddle

Parent Consent Form Template

Security and Privacy Certifications

ISO 27001, 27017, 27018, and 27701



Toddle holds the following four ISO certifications:

- **ISO/IEC 27001:2022**: The most rigorous global security standard for Information Security Management Systems (ISMS).
- **ISO/IEC 27017:2015**: Provides guidelines for information security controls applicable to the provision and use of cloud services.
- **ISO/IEC 27018:2019**: Establishes controls and guidelines for protecting Personally Identifiable Information (PII) in the public cloud.
- **ISO/IEC 27701:2019**: Specifies requirements and guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

Schools can obtain copies of the certificates from here.

SOC 2 Type II

Toddle has successfully completed the SOC 2 Type II audit, validating the effectiveness of its security, availability, and confidentiality controls. This certification, conducted by an independent third party, confirms that Toddle has implemented rigorous processes and practices to uphold the highest standards of security and data protection.

Schools can obtain a copy of the report from here.

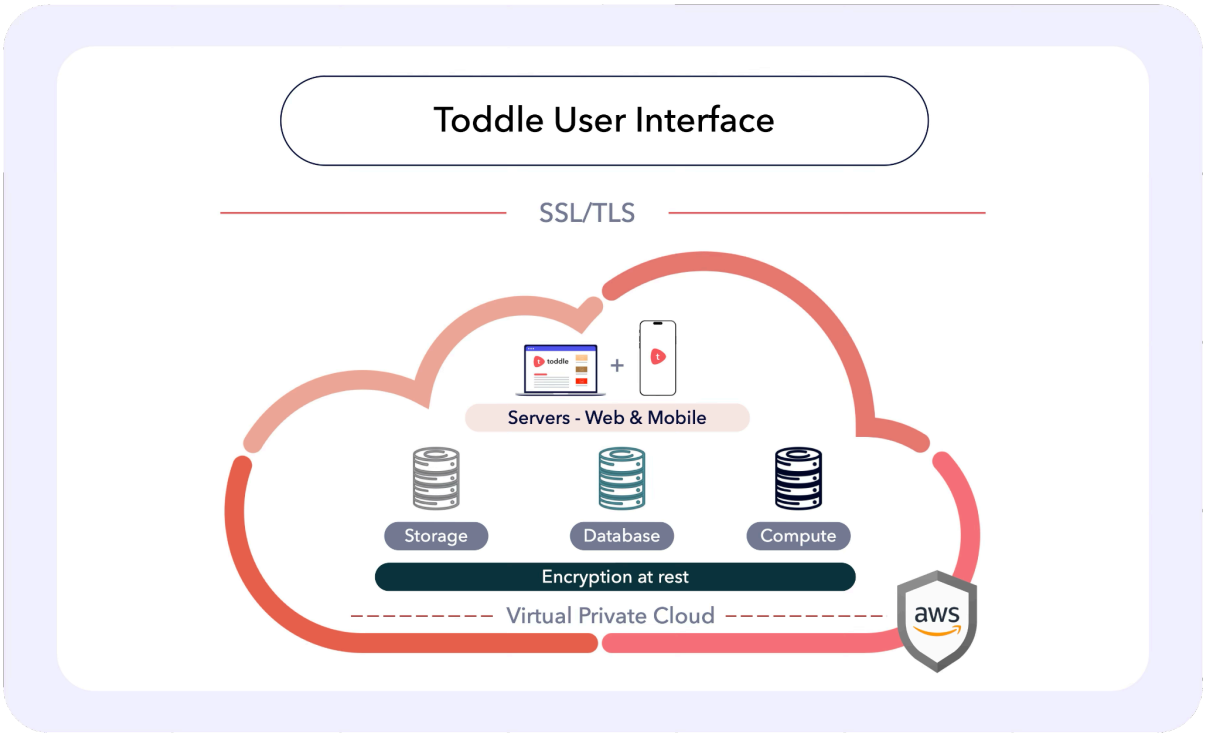
Infrastructure

Hosting Provider

Toddle is built on top of Amazon Web Services (SOC 1, SOC 2, and SOC 3 certified), a powerful and reliable cloud platform. This means that Toddle uses AWS's servers to store and process all of your data.

To provide its services, Toddle uses three main types of servers on AWS:

- **Storage servers**: This is where all media (photos, videos, files, etc.) are securely stored. All files are encrypted both during storage (at rest) and while being transferred (in transit). Toddle uses Amazon Web Services' S3 servers for this purpose.
- **Database servers**: This is a relational database that stores data in organized tables. Like the storage servers, all data in the database is also encrypted both in transit and at rest.
- **Compute servers**: Whenever a user interacts with Toddle, the compute servers handle processing these requests to ensure a smooth and responsive experience.



Datacenter Locations

Toddle offers multiple AWS data center locations to its customers who require their data to be stored in a specific location:

Region	Primary Data Center Location	Backup Location
Australia	Sydney	Melbourne
China	Beijing	Beijing
Europe	Ireland	Frankfurt
Singapore	Singapore	Tokyo
United Arab Emirates	Dubai	Dubai
United States of America	N. Virginia	Oregon

Note: For users in other regions, you can choose to store your data in any of the following locations: Australia, Ireland, Singapore, the United Arab Emirates, or the United States of America.

Toddle continues to expand its data storage options. Please check the Privacy & Security Center for updates.

Access to production

Access to Toddle's production environment is strictly controlled and granted only on a need-to-know basis, adhering to the principle of least privilege. Administrative privileges are exclusively reserved for a specialized team of experienced engineers within its Infrastructure Team with enforcement of robust password policies along with mandatory Multi-Factor Authentication (MFA).

Encryption and key management

Encryption in transit

All data in transit is protected by TLS 1.2+ encryption with strong ciphers. This is enforced for all connections to its servers, including web, API, mobile apps, and email access.

Encryption at rest

Data at rest is encrypted using AES-256. Encryption keys are stored using AWS Key Management Service (KMS).

Tenant Separation

Toddle's platform is designed to serve multiple customers securely, with strict logical boundaries in place to keep each customer's data completely separate. This is achieved through a unique identification system that assigns a combination of parameters to create unique IDs, ensuring data segregation at the application level.

Service Level Commitment

Toddle is committed to providing a reliable and secure service to its users. Service Level Commitment includes a server uptime guarantee of 99.9%.

Separate Production Environment

Toddle's development and testing environments are separate from the production environments. Customer data is never stored in non-production environments.

Virtual Private Cloud

Toddle utilizes AWS Virtual Private Cloud to ensure that all of their compute needs are done in a secured environment, separate from other public cloud tenants.

Backups

Toddle continuously takes backup of user data using automated schedulers. The backup is taken in a separate server location and encrypted using AES-256 bit algorithm.

Data Type	Backup Type	Frequency
Database (AWS)	Incremental Backup	Every 5 minutes (Automated)
	Full Backup	Daily (Automated) Monthly (Automated)

Application Security

Design Reviews

The security team at Toddle integrates security reviews into the product roadmap, ensuring that every major release undergoes threat modeling and design reviews to provide a secure experience for users.

Secure Deployment

As part of the software development lifecycle (SDLC), any new feature added to the Toddle application is rigorously analyzed for code quality and potential security vulnerabilities. Each feature must pass a comprehensive review process, including peer evaluations, before being approved for release.

Change Management

Toddle's change management process follows a formal policy developed by its Engineering team. This ensures that system modifications are properly tested and authorized before being implemented in the production environment. Developers initiate source code changes, which are stored in a version control system and must pass automated Quality Assurance (QA) testing to confirm compliance with security standards. Only after successful QA testing are these changes deployed into production, with logs maintained and alerts sent to the engineering management team.

All infrastructure changes are restricted to authorized personnel only, with the Toddle security team overseeing infrastructure security. This includes maintaining up-to-date servers, and ensuring configurations meet industry standards.

Web application firewall (WAF)

Toddle uses AWS WAF to protect its platform from common web exploits, ensuring a secure environment.

Vulnerability & Penetration tests

On an annual basis, Toddle brings a professional security assessment firm to thoroughly assess its web and mobile applications to identify any potential weaknesses. As part of Toddle's Information Security Management System (ISMS), all findings and recommendations from these assessments are reported to the management team, carefully reviewed, and appropriate actions are taken as necessary.

High-severity issues are thoroughly documented, tracked, and resolved by dedicated security engineers to ensure swift and effective remediation.

Schools can obtain a copy of the latest reports from Toddle's Trust Vault.

Rate limiting

Toddle has implemented rate limiting to safeguard its platform and users. This mechanism restricts the frequency of requests from a user or IP address within a defined timeframe, effectively mitigating threats like denial-of-service attacks, brute-force attempts, and API abuse. Toddle's calibrated rate limits strike a balance between security and user experience, ensuring legitimate access while deterring malicious activity. These limits are continuously monitored and adapted to address evolving threats and usage pattern

Operational security

Toddle Information Security

Toddle maintains a formal information security management program with a dedicated team of security specialists, reporting directly to Toddle's Chief Information Security Officer. This team is responsible for implementing and maintaining strong security measures, as well as actively monitoring Toddle's systems for any potential threats, ensuring a safe and secure experience for all users.

Human Resources

“Hire right, set the expectations from the beginning, train well, review from time to time, and close the loop at the exit.”

Background checks

All personnel hired by Toddle undergo thorough background checks, adhering to industry best practices and complying with relevant laws and regulations.

Employment Terms

At Toddle, every employment contract includes strict confidentiality clauses and provisions that allow for immediate termination in cases of specific breaches of duties or commitments. In addition, Toddle upholds a comprehensive HR security policy that outlines the necessary security measures and responsibilities throughout an employee's tenure, from recruitment to departure.

Acceptable use

Toddle has a strict policy on acceptable use that is carefully reviewed every year by its security experts. Toddle make sure all employees understand and agree to this policy, either when they first join or whenever the policy changes significantly.

Training Program

As part of the employee onboarding process, all personnel complete Information Security training based on the Privacy Skill Matrix defined by Toddle. This training covers a wide range of topics, including data protection, phishing awareness, password hygiene, and incident response. To reinforce these concepts, Toddle sends monthly emails with security and privacy tips, ensuring these topics remain top of mind for everyone. Additionally, yearly refresher sessions are conducted to keep all employees up to date with the latest security practices and protocols.

Termination

Upon exit, all access to Toddle information is revoked within 1 business day for the departing employee.

User Access Reviews and Policy

Toddle is proactive in managing access to its systems. Every month, the management team reviews user access to ensure it remains appropriate and removes any access that is no longer needed.

Data Center Security

Toddle leverages AWS's robust physical and environmental controls, which are implemented in state-of-the-art facilities independently assessed through third-party audits, including SOC 1, SOC 2, and ISO 27001 certifications. Amazon consistently manages risk and undergoes regular evaluations to maintain compliance with industry-leading standards. For further details on their security practices, please visit AWS Security Compliance.

Governance and Risk management

Toddle has a dedicated Governance, Risk, and Compliance (GRC) team, supported by a comprehensive GRC platform to efficiently manage the ongoing risk assessment process. This team is responsible for proactively identifying vulnerabilities within Toddle's systems, evaluating new and emerging threats to the company's operations, and reviewing procedures and policies in Toddle to ensure alignment with industry standards. They determine the necessary controls, processes, and systems to meet these standards, conduct periodic internal audits, and facilitate independent audits and assessments by third parties.

Incident Response and Management

Toddle's robust incident response framework includes comprehensive policies and procedures designed to swiftly and effectively address issues related to service availability, data integrity, security, privacy, and confidentiality. The incident response procedures involve specialized teams who are prepared to:

- **Immediate Response**: Quickly react to alerts signaling potential incidents.
- **Incident Assessment**: Evaluate the severity and scope of the incident.
- **Mitigation & Containment**: If required, initiate appropriate measures to mitigate and contain the impact.
- **Evidence Collection**: Secure and preserve any evidence for further investigation.
- **Post-Incident Analysis**: Document the findings, create a postmortem report, and develop long-term strategies to prevent recurrence.

These incident response procedures are regularly audited as part of its SOC 2, ISO/IEC 27001, and other security compliance assessments.

Notification

Toddle will promptly address any security incidents and notify affected parties under applicable laws and timelines, ensuring timely communication.

Country	Notification Timeline	Law/Regulation
Argentina	Immediately	Personal Data Protection Law (PDPL)
Australia	30 days of becoming aware	Notifiable Data Breaches (NDB) scheme
Brazil	Within a reasonable time	General Data Protection Law (LGPD)
Canada	As soon as feasible	Personal Information Protection and Electronic Documents Act (PIPEDA)
China	Without undue delay	Cybersecurity Law of the People's Republic of China
Colombia	As soon as possible	Law 1581 of 2012
Egypt	Within 24 hours	Personal Data Protection Law
European Union	Within 72 hours	General Data Protection Regulation (GDPR)
Hong Kong	As soon as practicable	Personal Data (Privacy) Ordinance (PDPO)
Iceland	Within 72 hours	Data Protection Act (implementing GDPR)
India	6 hours of noticing the incident	CERT-In Rules 2013
Indonesia	Without undue delay	Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions
Israel	As soon as possible	Protection of Privacy Regulations (Data Security) 2017
Japan	Without delay	Act on the Protection of Personal Information (APPI)
Malaysia	Within 72 hours	Personal Data Protection Act 2010
Mexico	As soon as the breach is confirmed	Federal Law on Protection of Personal Data Held by Private Parties
New Zealand	As soon as practicable	Privacy Act 2020
Norway	Within 72 hours	Personal Data Act (implementing GDPR)
Philippines	Within 72 hours	Data Privacy Act of 2012
Russia	Without undue delay, no more than 3 days	Federal Law on Personal Data
Saudi Arabia	Without undue delay	Personal Data Protection Law

Country	Notification Timeline	Law/Regulation
Singapore	As soon as practicable, no later than 3 days	Personal Data Protection Act (PDPA)
South Africa	As soon as reasonably possible	Protection of Personal Information Act (POPIA)
South Korea	Within 24 hours	Personal Information Protection Act (PIPA)
Switzerland	As soon as possible	Federal Act on Data Protection (FADP)
Taiwan	Within 72 hours	Personal Data Protection Act (PDPA)
Thailand	Within 72 hours	Personal Data Protection Act (PDPA)
Turkey	Without undue delay	Personal Data Protection Law (KVKK)
UAE	Without undue delay	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data
United Kingdom	Within 72 hours	Data Protection Act 2018 (DPA 2018) / GDPR
United States	Varies by state, generally 30-60 days	State-specific Data Breach Notification Laws
Vietnam	Within 72 hours	Law on Cybersecurity
All other countries	As soon as reasonably possible/feasible depending on local regulations	Local Data Protection Laws

Disaster Recovery and Business Continuity

Toddle's Business Continuity Plan (BCP) is designed to handle unexpected disruptions, ensuring critical systems are quickly restored. Using AWS's CloudEndure disaster recovery system, Toddle can recover data within a 3-hour window (RTO) and with a 5-minute Recovery Point Objective (RPO), even in the event of a complete database crash. During such events, service levels and turnaround times will be temporarily paused, and the Business Continuity Team will oversee the response. Toddle also conducts annual testing of its disaster recovery plan, sharing the results with customers for transparency.

Data Retention and Disposal

Data Retention

Toddle will retain your information throughout the contract term. After contract termination, it will be retained for 7 years or as long as necessary to fulfill the purposes outlined in its Privacy Policy. Data that Toddle processes on behalf of its customers will be retained under Toddle's Terms of Service, Toddle's Data Processing Agreement, as mandated by law, and any other relevant agreements.

Data Deletion

You have the right to "forget ability", i.e., Toddle will remove all your information from its systems if you so wish. If you would like to delete your Toddle account or any content submitted to Toddle, please send an email to privacy@toddleapp.com. Toddle will notify you by email before deleting your account from its database. After receiving your request, Toddle may still retain information for up to 365 days to provide customer support and prevent accidental deletion.

Toddle provides a Data Deletion Certificate upon request. This certificate confirms that the deletion process has been completed, which can be used as evidence during audits or compliance checks.

For users in the USA, please note that to comply with FERPA, Toddle may need to retain certain student education records once a valid request to inspect those records has been made and Toddle may retain your data to comply with the FERPA requirements.

Data Destruction

Toddle leverages Amazon Web Services (AWS) for its service hosting. AWS employs robust data distribution and deletion strategies to safeguard sensitive information in a multi-tenant environment. When storage media is decommissioned, AWS adheres to the rigorous techniques outlined in NIST 800-88 to ensure data security.

Monitoring and Logs

Toddle uses Amazon CloudWatch and Cloudtrail, combined with custom scripts that extract important data from logs and push them to its monitoring services. Toddle monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure service delivery matches service level agreements.

Application and server logs are retained in CloudWatch for 3 years. Other monitoring logs for the machines are stored for one week.

Third-Party Service Providers

Toddle carefully selects and partners only with third-party service providers who adhere to security measures that align with its stringent policies. Before any software is implemented or a vendor is used, Toddle's GRC team conducts a thorough review of the vendor's security protocols, data retention policies, privacy policies, and overall security track record. Toddle only works with vendors who can demonstrate their ability to protect Toddle's data and users. Additionally, Toddle requires all third-party service providers to sign a written agreement that includes data protection obligations at least as robust as the technical and organizational measures Toddle has in place. Toddle conducts annual re-evaluations of its critical vendors to ensure they continue to meet its high standards.

To review Toddle’s current list of third-party service providers, visit here

IT security

Endpoint security

All endpoints at Toddle run the latest OS version and are equipped with a centrally managed Endpoint Detection and Response (EDR) solution with Extended Detection and Response (XDR) capabilities (SentinelOne), constantly monitored by a 24/7 Security Operations Center (SOC) team to promptly identify and isolate malware threats. Devices are equipped with FileVault/BitLocker encryption, password protection, and automatic screen timeouts. Toddle also has the capability to remotely apply patches or wipe devices with the help of an enterprise Mobile Device Management (MDM) solution (Scalefusion), ensuring continuous protection and control over its endpoints.

Password protection

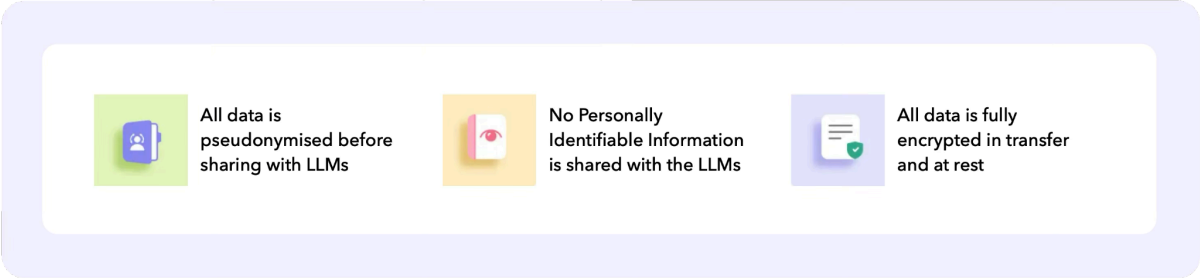
Password Guidelines for all Toddle employees

- All passwords must be 8 characters long
- The passwords must at least contain one numeral, one special character, and one alphabet
- The passwords must be changed every 60 days
- The passwords cannot be the same as the user name
- Do not use common passwords such as reset, admin, etc.
- Do not use personal information in passwords such as date of birth, name, etc.
- Do not share your password with anyone, and do not give access to your accounts to anyone else
- Do not reveal your password over a phone, or email, to anyone
- Do not write the passwords and store them anywhere

Email Protection

Toddle uses Google Workspace as its email provider. DMARC and SPF are in place. Toddle provides ongoing training to all employees on how to identify and avoid phishing attempts, and regularly tests their knowledge to ensure they're prepared for real-world scenarios.

Data Privacy with Toddle AI



All of our AI use cases run entirely within Toddle's own infrastructure, this means that instead of relying on external providers to run our AI features, we process them within our own secure infrastructure, ensuring that your data never leaves **Toddle's trust boundaries** and hence is never shared with any third party LLM companies**.**

Our current LLM providers, which are also listed in our **Subprocessor List**, include:

Amazon Bedrock (listed as Amazon Web Services, Inc.) – Utilizing Anthropic's model 'Claude' within AWS's infrastructure, managed under Toddle's own AWS account, with available locations including USA, Ireland, Singapore, or Australia, ensuring enhanced control and security.

Microsoft's Azure OpenAI - utilizing OpenAI models within the Microsoft infrastructure in USA/Sweden to deliver certain features.

By **regionally hosting these models within the United States and Europe**, we ensure our customers' data remains within its designated region. This allows us to maintain strict

control over data residency, comply with local regulations, and securely manage all AI use cases end-to-end.

Toddle does not use any User-Generated Data for the training or development of Large Language Models (LLMs) or similar AI systems. All User-Generated Data is collected solely for the purpose of providing and improving the Service Provider's services, in strict adherence to its Privacy Policy.

AI Security and Safety Measures

Security Testing

Penetration & Jailbreak Testing: We regularly challenge our AI's security controls to identify any paths bad actors might exploit to alter or misuse the system.

Vulnerability Scanning: Automated scans help us pinpoint and promptly remediate any weaknesses in our AI integrations.

Access Control Checks: We verify that only authorized users can access Toddle AI features and that user-level permissions are being properly enforced.

Safety Testing

Bias & Fairness Analysis: We continuously evaluate AI outputs to ensure they are free from discriminatory patterns.

Explainability Verification: We test whether AI responses are clear, interpretable, and aligned with established educational best practices.

Edge Case Validation: We simulate rare or unpredictable scenarios to ensure Toddle AI behaves responsibly even under unusual conditions.

Content & Interaction Integrity Checks: We confirm that the AI's responses remain appropriate, contextually relevant, and safe.

Inappropriate Content Generation Testing: We actively monitor for and block harmful, misleading, or inappropriate outputs.

Privacy Policy and Compliance

Privacy Policy

Toddle's Privacy Policy details its current data practices and is regularly updated to reflect any changes. This document outlines the information Toddle collects and processes, as well as how individuals can exercise their privacy rights under applicable laws.

Key points:

- Toddle collects personal information such as name, email, and usage data for account creation, service improvement, and personalization.
- Data is used to enhance services, analyze trends, and communicate with users.
- Data is shared with third parties for service enhancement, legal compliance, and user consent.
- Users can access, update, correct, or delete their data, and restrict certain processing activities.
- Toddle does not share data for advertising purposes.
- Toddle never sells data to anyone for any purpose.
- Cookies are used to enhance user experience and provide personalized content.
- Data is retained as long as needed for outlined purposes or as required by law.
- Toddle complies with GDPR, COPPA, FERPA, CCPA, DPDPA, APPs, PDPL, and other privacy laws.
- Toddle protects children's privacy with parental consent and strict data handling.
- Data transferred across borders is protected per international standards.
- Users are notified of significant privacy policy changes.

Compliance

Compliance with FERPA

Toddle partners with and is certified by **iKeepSafe** for compliance with FERPA.

FERPA is the “Family Education Rights and Privacy Act”. It governs the terms to protect personally identifiable information (PII) of students. Data collected by Toddle may include personally identifiable information from “education records” (Education Records in FERPA refers to documents, digital or otherwise, that may contain information related to a student and maintained by an educational agency).

Toddle will abide by the following:

- Student records obtained by Toddle from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights to the personal information and education records it provides to Toddle.
- Toddle users may retain possession and control of their own generated content on Toddle Services.
- Toddle will not use any information in a student record for any purpose other than those required or specifically permitted by Toddle’s Terms of Use and Privacy Policy.
- Parents, legal guardians, or eligible students may review personally identifiable information in the student’s records and correct erroneous information by contacting their educational institution. Additionally, Toddle users may access, correct, update, or delete personal information in their profile by signing into the Toddle App/ Web platform, accessing their Toddle account, and making the appropriate changes.
- Toddle is committed to maintaining the security and confidentiality of student records. Towards this end, Toddle takes the following actions: (a) limit employee access to student data to only those employees with a need for such access to fulfill their job responsibilities; (b) conduct background checks on its employees that may have access to student data; (c) conduct regular employee privacy and data security training and education; and (e) protect personal information with technical,

contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.

- In the event of an unauthorized disclosure of a student's records, Toddle will (1) promptly notify Users unless specifically directed not to provide such notification by law enforcement officials. The notification shall identify: (i) the date and nature of the unauthorized use or disclosure; (ii) Private Data used or disclosed; (iii) general description of what happened, including who made the unauthorized use or received the unauthorized disclosure; (iv) what Toddle has done or shall do to mitigate any effect of the unauthorized use or disclosure; (v) what corrective action Toddle has taken or shall take to prevent future similar unauthorized use or disclosure; and (vi) who at Toddle the User can contact. Toddle will keep the User fully informed until the incident is resolved.
- Toddle will delete or de-identify personal information when it is no longer needed, upon expiration or termination of its agreement with an educational institution with any deletion or de-identification to be completed according to the terms of Toddle's agreement with the educational institution, or at the direction or request of the educational institution.
- Toddle agrees to work with the educational institution to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians, or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described in statement (4) above.
- Toddle prohibits using personally identifiable information in student records to engage in targeted advertising.

Compliance with COPPA

Toddle partners with and is certified by **iKeepSafe** for compliance with COPPA.

As a third-party operator, Toddle relies on School Consent for all underage children under COPPA. Toddle operates as a School Official under the FERPA regulations and complies with these regulations as they relate to children under the age of 13. If you are a school or teacher and you would like to obtain direct parental consent from the parent, Toddle has provided a consent form which can be downloaded here. Toddle does not encourage children to share their work publicly. Toddle continuously reviews and updates its practices to ensure compliance with COPPA requirements.

Toddle will abide by the following:

- As a third-party operator, Toddle relies on School Consent for all underage children under COPPA. Toddle operates as a School Official under the FERPA regulations and complies with these regulations as they relate to children under the age of 13. If you are a school or teacher and you would like to obtain direct parental consent from the parent, Toddle has provided a consent form which can be downloaded here.
- Student accounts in Toddle can only be created by the teachers. Teachers can generate a unique code for every student and the student, using that unique code, can log in into their account for the first time. Once logged in, they can set their own secure password.
- Toddle will delete an account and all content associated with the account if the account has not been accessed for more than 1 year. Prior to deleting an abandoned account, Toddle will notify the teacher or school associated with the account by email and provide an opportunity to download an archive copy of the related class journal.
- If you would like to delete your Toddle account or any content submitted to Toddle, please send an email to privacy@toddleapp.com. If you request that your account or any content submitted to Toddle be deleted, Toddle may still retain information for up to 365 days to provide customer support and prevent accidental deletion. An Email will still be sent to you before the information is completely removed from its databases.

- If you are a teacher or school administrator within the US, please be aware that FERPA requires us to retain student education records once a valid request to inspect those records has been made.
- In order to help Toddle provide, maintain, protect, and improve its services, Toddle shares information with other partners, vendors, and trusted organizations to process it on its behalf in accordance with its instructions, Privacy Policy, and any other appropriate confidentiality, security or other requirements Toddle deems appropriate. These companies will only have access to the information they need to provide Toddle services. You can get more details on the third-party service providers here.
- Toddle may send Push Notifications to its users. These push notifications will be sent and controlled by the teachers or school administrators. Toddle may send usage-related push notifications.
- Toddle does not encourage children to share their data publicly. Teachers and the school control the visibility of the data. The class journal is by default private to a classroom.

Compliance with GDPR

Data Processing Agreement

Toddle offers a Data Processing Agreement to all its users located in the EU/EEA and Switzerland. This Data Processing Agreement is signed at the time of the school's onboarding with Toddle. You can request a copy of the DPA by writing to privacy@toddleapp.com.

How does Toddle comply with GDPR?

- **Lawfulness, Fairly, and Transparency**: All data processing that Toddle does is lawful and is clearly called out in its privacy-related policies.
- Purpose Limitation: Toddle only uses your data for the purposes clearly specified in the contract.
- **Data Minimisation**: Toddle collects minimal data – only data that is needed to provide you with services agreed upon in the contract.
- Integrity and confidentiality: Toddle follows industry best practices to ensure that all your data is stored safely and securely. All your data is encrypted at rest and in transit.
- **Ownership of data**: All the data that you add to Toddle belongs to you and you have full rights over it.
- **Parental Consent**: For children below the age of 16, schools should collect explicit parental consent for the usage of Toddle. You can download the parental consent form from Toddle.
- **Right of Access**: You can reach out at any time to see your personal data and how it is processed.
- **Right to Rectification**: Toddle does its best to ensure that all data on Toddle is accurate, however, if you want to edit, modify, delete, or in any other way change any of your personal data, please reach out to privacy@toddleapp.com.
- **Right to be forgotten**: If you do not wish to use Toddle services anymore and want all of your data deleted from its records, please reach out to the Toddle's team and Toddle will delete all of your information from all of its records.

- **Right to data portability**: All data that you add to Toddle belongs to you and should you want to receive that data, Toddle will provide you with a machine-readable format of the same within 1 month of receiving such a request.
- **Toddle employees**: All Toddle employees get periodically trained in relevant data security practices. All employees undergo a relevant background check, sign a non-disclosure agreement, and immediately lose access to all systems and data when terminated.

Contact:

Toddle's Data Protection Officer is Anshul Chauhan. In case of any questions/ queries, please reach out to privacy@toddleapp.com.

In compliance with Article 27 of the General Data Protection Regulation (GDPR), we have appointed Rickert Rechtsanwaltsgesellschaft mbH as our representative in the European Union for matters concerning data protection. You may contact our EU GDPR Representative directly using the following details:

Name: Rickert Rechtsanwaltsgesellschaft mbH
– Teacher Tools Private Limited –
Address: Colmantstraße 15, 53115 Bonn, Germany
Email: art-27-rep-toddle@rickert.law

Compliance with DPDPA

Toddle is committed to complying with the Digital Personal Data Protection Act, 2023 (DPDPA), a comprehensive legislation that governs the collection, use, storage, and disclosure of personal data in India.

How Toddle Protects Your Data Under DPDPA

Lawful Processing

Toddle collects and processes your personal data only for specified, legitimate purposes outlined in its comprehensive Privacy Policy.

Security Measures

Your data security is Toddle's priority. Toddle uses robust security measures to protect your personal information from unauthorized access, changes, or misuse. Toddle continuously adapts its practices to stay ahead of new threats.

Data Breach Notification

In the event of a personal data breach that is likely to cause harm to the Data Principal(s), Toddle will promptly notify the affected Data Principal(s) and report the breach to the Data Protection Board of India within 72 hours of becoming aware of the breach, in accordance with the Digital Personal Data Protection Act, 2023. Toddle will also take immediate steps to mitigate risks and prevent further harm.

Parental Consent

Toddle understands the importance of protecting the privacy of children (defined as individuals below the age of 18). As a Data Processor under the Digital Personal Data Protection Act, 2023 (DPDPA), Toddle processes data only on the instructions of the Data Fiduciary (typically the school/teacher). The Data Fiduciary is responsible for obtaining verifiable parental consent before sharing any child's personal data with us. To support this process, Toddle has provided a consent form which can be downloaded from here.

Right of Access

You can reach Toddle at any time to see a summary of all your personal data being processed along with the related processing activities. You can also request the identity of any third-party Data Processors and Data Fiduciaries with whom your personal data has been shared.

Right to Correction, Updation & Completion

Toddle respects your right to have accurate and complete information. If you find that any personal data Toddle holds is inaccurate, incomplete, or needs updating, you can request its correction, updation, or completion by contacting privacy@toddleapp.com.

Right to Erasure

If you no longer wish to use Toddle's services and want your data deleted from its records, please contact Toddle's team, and Toddle will delete all of your information from its records unless Toddle is legally required to retain certain data.

Right of Grievance Redressal

If you have any questions or concerns about your data privacy rights under the DPDPA, you can reach out to Toddle's Data Protection Officer, Anshul Chauhan, at privacy@toddleapp.com.

Right to Nominate an agent

The DPDPA recognizes your right to appoint a representative to manage your data privacy rights in case of death or incapacitation. Toddle will uphold your designated representative's authority.

Compliance with CCPA

As a service provider, Toddle is dedicated to complying with the California Consumer Privacy Act (CCPA). Toddle actively adapts to evolving industry standards to ensure its customers can continue using Toddle seamlessly while adhering to CCPA requirements when processing the personal information of California consumers.

How does Toddle comply with CCPA?

Right to Know

Toddle recognizes your right to know what personal information Toddle collects and how it's used. Toddle's Privacy Policy outlines the categories of personal information collected, the sources, purposes for collection, and the third parties with whom this information may be shared. Individuals can request a detailed report of their personal information by contacting privacy@toddleapp.com.

Right to Delete

If you no longer wish to use Toddle's services and want your data deleted from its records, please contact Toddle's team, who will delete all of your information from its records unless Toddle is legally required to retain certain data.

Right to Opt-Out of Sale

Toddle does not sell your personal information.

Right to Non-Discrimination

Toddle will not discriminate against you if you exercise any of your rights under the CCPA. You will continue to have the same access to its services and features regardless of your decision to exercise these rights.

Right to Limit

Toddle only uses your data for the purposes clearly specified in the contract.

Right to Correct Information

Toddle respects your right to have accurate and complete information. If you find that any personal data Toddle holds is inaccurate, incomplete, or needs updating, you can request its correction, updation, or completion by contacting privacy@toddleapp.com.

Parental Consent

For children below the age of 13, schools should collect explicit parental consent for the usage of Toddle. You can download the parental consent form from here.

Authorized Agents

You can designate an authorized agent to make a request on your behalf. Toddle will uphold your designated agent's authority. Toddle may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.

Data Security

Toddle adheres to the internationally recognized standards of the International Organization for Standardization (ISO) and holds ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 & ISO/IEC 27701:2019 certifications.

Toddle is certified by iKeepSafe for data protection laws under COPPA and FERPA and has also successfully completed a SOC 2 Type II audit. All your data is encrypted in transit and at rest, and stored on Amazon Web Services servers in the US. All of Toddle's personnel undergo data security training.

Compliance with KSA PDPL

Data Processing Agreement

Toddle offers a Data Processing Agreement to all its users located in the KSA. This Data Processing Agreement is signed at the time of the school's onboarding with Toddle. You can request a copy of the DPA by writing to privacy@toddleapp.com.

How Toddle Protects Your Data Under PDPL

Lawfulness, Fairness, and Transparency

Toddle collects and processes your personal data only for specified, legitimate purposes outlined in our comprehensive Privacy Policy.

Purpose Limitation

We only use your data for the purposes clearly specified in the contract.

Data Minimization

We collect minimal data – only data that we need to provide you with services agreed upon in the contract.

Storage Limitation

Personal data is retained only as long as necessary to achieve the intended purposes specified in the contract.

Confidentiality and Security

We follow industry best practices to ensure that all your data is stored safely and securely. All your data is encrypted at rest and in transit.

Accountability

We are committed to complying with PDPL and maintain records of our data processing activities to demonstrate our adherence to these principles.

Data Breach Notification

In the event of a personal data breach that poses a risk to the rights and freedoms of Data Subjects, Toddle will notify the Data Controller without undue delay, and no later than 24 hours after becoming aware of the breach. We will also support the Data Controller in notifying the relevant authority, SDAIA, within 72 hours, if required.

Data Protection Impact Assessments (DPIAs)

We support Data Controllers in conducting DPIAs for processing activities that may pose high risks to Data Subjects' rights and freedoms.

Data Transfers

Our customers have the flexibility to choose where their data is hosted, with options including Australia, Ireland, Singapore, United Arab Emirates, and the United States of America. All transfers of personal data to these data centers are conducted in strict accordance with the contract signed with the Data Controller and in full compliance with the requirements of the Personal Data Protection Law (PDPL).

Parental Consent

Toddle collects user data after receiving their consent. Schools are responsible for obtaining verifiable parental consent for using Toddle for children below the age of 13. If you come across an instance where Toddle is collecting information from a student without parental consent, please contact us immediately at privacy@toddleapp.com. Schools can download a sample of the Parental Consent form from here.

Your Rights Under PDPL

Right to Access

You can reach Toddle at any time to see a summary of all your personal data being processed along with the related processing activities.

Right to Correction, Updation & Completion

Toddle respects your right to have accurate and complete information. If you find that any personal data we hold is inaccurate, incomplete, or needs updating, you can request its correction, updation, or completion by contacting privacy@toddleapp.com. Users can also update their information from the Profile sections on the platform and the applications.

Right to request Destruction

If you no longer wish to use Toddle's services and want your data deleted from our records, please contact our team, and we will delete all of your information from our records unless we are legally required to retain certain data.

Right to Restrict Processing

If you wish to limit how your personal data is processed, please reach out to our team. We will implement the necessary restrictions on processing your data in accordance with PDPL requirements.

Right to Obtain

You can request a copy of your personal data in a structured, commonly used, and machine-readable format. We will facilitate the transfer of your data.

Right to Withdraw Consent

If processing is based on your consent, you have the right to withdraw that consent at any time. Simply contact us or the Data Controller, and we will cease processing your data as per your request.

Right to Be Informed

You have the right to be informed about how your personal data is being collected, used, and processed. Toddle ensures full transparency in all data-related activities.

Contact

If you have any questions about your personal data, or if you would like to exercise any of your rights under PDPL, please contact our Data Protection Officer, Anshul Chauhan, at privacy@toddleapp.com.

Compliance with HK PDPO

Under the Hong Kong's PDPO, there are 6 Data Protection Principles (DPPs) that set out the baseline requirements for personal data privacy protection in Hong Kong:

- **DPP1:** Purpose and manner of collection of personal data
- **DPP2:** Accuracy and retention of personal data
- **DPP3:** Use of personal data
- **DPP4:** Security of personal data
- **DPP5:** Information to be generally available
- **DPP6:** Access to personal data

Below, we detail how Toddle ensures compliance with each of these principles.

DPP1 – Purpose and Manner of Collection of Personal Data

Toddle collects personal data in a fair and lawful manner, and only when it is necessary for us to provide our services effectively. The types of data we collect, and the purposes for which they are used, are clearly explained in our Privacy Policy.

DPP2 – Accuracy and Retention of Personal Data

Toddle ensures the accuracy and proper retention of personal data. All personal data is added directly by schools using the platform, and Toddle does not independently input or modify any user information. If users identify inaccuracies or require corrections, they can easily update their data directly via their Toddle accounts. If they find any inconsistencies, they can email us at privacy@toddleapp.com. We retain personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by law.

DPP3 – Use of Personal Data

Toddle ensures that personal data is used strictly for the purposes explicitly outlined in the contract with schools. Any changes to our data usage practices or Privacy Policy that materially affect users' privacy rights are communicated to users at least 30 days in advance, ensuring transparency and providing sufficient time for review. Users who have concerns or questions about these changes can contact us directly at privacy@toddleapp.com. Toddle does not sell or share user data with external marketing agencies and limits data sharing to trusted sub-processors as required for delivering services, in strict compliance with the agreed terms.

DPP4 – Security of Personal Data

Toddle is committed to safeguarding personal data against unauthorized or accidental access, processing, or erasure. We adhere to internationally recognized security standards, holding certifications such as ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019, and ISO/IEC 27701:2019. Additionally, Toddle has successfully completed a SOC 2 Type II audit, demonstrating our strict control environment for data security, availability, and confidentiality.

Our platform complies with key regulations, including COPPA (Children's Online Privacy Protection Act), FERPA (Family Educational Rights and Privacy Act), and GDPR (General Data Protection Regulation), ensuring robust privacy protections for users worldwide. Personal data is encrypted both in transit and at rest and is stored securely on Amazon Web Services (AWS) servers.

Toddle's personnel undergo comprehensive data security training to ensure the highest standards of data protection. In the event of a data breach, we will promptly act to contain the issue, notify affected users, and inform relevant authorities, as required by applicable laws and regulations.

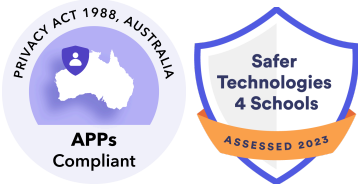
DPP5 – Information to Be Generally Available

Toddle adopts a very transparent approach towards its Privacy Practices. The Privacy Policy, Terms of Use and Terms of Service are all hosted on its website www.toddleapp.com. Toddle also has a designated Data Protection Officer, Anshul Chauhan and he can be contacted at privacy@toddleapp.com.

DPP6 – Access to and Correction of Personal Data

Toddle respects users' rights to request access to and correction of their personal data. Upon receiving a valid request, we provide a summary of the personal data we process and how it is used, typically within 30 days. If any information is inaccurate, incomplete, or out of date, users may request corrections by emailing privacy@toddleapp.com or directly through their Toddle accounts. We also honor requests for data deletion unless we are legally required to retain certain information.

The Australian Privacy Act (APA) and Australian Privacy Principles (APPs)



The Australian Privacy Principles can be summarised in 13 broad points. These are:

- **APP 1:** Open and transparent management of personal information
- **APP 2:** Anonymity and pseudonymity
- **APP 3:** Collection of solicited personal information
- **APP 4:** Dealing with unsolicited personal information
- **APP 5:** Notification of the collection of personal information
- **APP 6:** Use or disclosure of personal information
- **APP 7:** Direct marketing
- **APP 8:** Cross-border disclosure of personal information
- **APP 9:** Adoption, use, or disclosure of government-related identifiers
- **APP 10:** Quality of personal information
- **APP 11:** Security of personal information
- **APP 12:** Access to personal information
- **APP 13:** Correction of personal information

Below we detail how we comply with all 13 principles.

APP 1- Open and Transparent Management of Personal Information

Toddle adopts a very transparent approach towards its Privacy Practices. The Privacy Policy, Terms of Use, and Terms of Service are all hosted on its website www.toddleapp.com. Toddle also has a designated Data Protection Officer, Anshul Chauhan and he can be contacted at privacy@toddleapp.com.

APP 2- Anonymity and Pseudonymity

Where practicable, Toddle provides individuals with the option of not identifying themselves or using a pseudonym. However, this may not always be possible for Toddle to provide its services effectively.

APP 3- Collection of Solicited Personal Information

Toddle collects minimal data from its users and the data collected is used only for providing the services that Toddle has with the user. For details on the types of personal information Toddle collects, how it is collected, and the use of cookies and tracking technologies, please refer to Toddle's Privacy Policy.

Toddle collects user data after receiving their consent. Schools are responsible for getting verifiable parental consent for using Toddle for children below legal age (as specified by the local laws). In case you come across an instance where Toddle is collecting information from a student without parental consent, please contact Toddle immediately at privacy@toddleapp.com. Schools can download a sample of the Parental Consent form from here.

APP 4- Dealing with Unsolicited Personal Information

If Toddle receives unsolicited personal information, Toddle will determine whether it could have been collected through normal means. If not, Toddle will destroy or de-identify the information as soon as practicable, provided it is lawful and reasonable to do so.

APP 5- Notification of the Collection of Personal Information

The collection of personal information on the Toddle platform is primarily managed by the schools that use Toddle services. Schools provide Toddle with the necessary data to set up and manage accounts for students, teachers, and parents.

Account creation in Toddle can happen in 3 ways:

1. Account for a teacher created by the teacher's school - Teachers can log in to their accounts as soon as they're ready.
2. Account for a student created by the school - This is governed by Parental Consent being collected by the school.
3. Teacher creating his/ her own account - A verification code is sent in an email to the teacher's email ID. The account is created only if the verification code is entered by the teacher.

APP 6- Use or Disclosure of Personal Information

Toddle only uses or discloses your data for the purposes specified in its agreement with you or your school, or as otherwise permitted by the APPs.

APP 7- Direct Marketing

Toddle does not sell or share data with marketing firms. Toddle also does not show any ads on any of its websites/ services. Toddle collects log data of visitors to its website www.toddleapp.com and web.toddleapp.com. Toddle may use this log data for marketing its own products to the visitors of its website.

APP 8- Cross-border Disclosure of Personal Information

Toddle shares user data with a limited set of third parties (sub-processors) to operate and improve Toddle. All of these sub-processors are contractually prohibited from sharing the user data with any other entity. You can see details of all the sub-processors used by Toddle on Toddle's website: Third Party Service Providers | Toddle

APP 9- Adoption, Use or Disclosure of Government-Related Identifiers

Not applicable, as Toddle does not adopt, use, or disclose government-related identifiers.

APP 10- Quality of Personal Information

If you find that any personal data Toddle holds is inaccurate, incomplete, or needs updating, you can request its correction by emailing privacy@toddleapp.com. Users can also update their information from the Profile sections on the platform and the applications.

APP 11- Security of Personal Information

Toddle adheres to the internationally recognized standards of the International Organization for Standardization (ISO) and holds ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 & ISO/IEC 27701:2019 certifications.

Toddle has successfully qualified to be part of the Safer Technologies 4 Schools (ST4S) Product Badge Program in 2024, covering our entire platform, including Toddle AI, is certified by iKeepSafe for data protection laws under COPPA and FERPA, and has also successfully completed a SOC 2 Type II audit. All your data is encrypted in transit and at rest, and stored on Amazon Web Services servers in Sydney. All of Toddle's personnel undergo data security training.

If you no longer wish to use Toddle's services and want your data deleted from its records, please contact Toddle's team, and Toddle will delete all of your information from its records unless it is legally required to retain certain data.

APP 12- Access to Personal Information

All data that you add to Toddle belongs to you. You can reach Toddle at any time to see a summary of all your personal data being processed along with the related processing activities. You can also request the identity of any third party with whom your personal data has been shared. Should you want to receive that data, Toddle will provide you with a machine-readable format of the same within 30 days of receiving such a request.

APP 13- Correction of Personal Information

Toddle respects your right to have accurate and complete information. If you find that any personal data Toddle holds is inaccurate, incomplete, or needs updating, you can request its correction, updation, or completion by contacting privacy@toddleapp.com. Users can also update their information from the Profile sections on the platform and the applications.

Notifiable Data Breaches (NDB) Scheme

The NDB scheme mandates that Toddle must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach occurs that is likely to result in serious harm to any individual whose personal information is involved. If Toddle experiences such a breach, Toddle will take immediate steps to contain it and assess the risk of harm. Affected individuals will be notified with a description of the breach, the types of information involved, and recommended steps they can take to protect themselves. Additionally, Toddle will notify the OAIC and provide details of the breach and its response. Toddle is dedicated to ensuring the security of your personal information and will take all necessary actions to prevent and respond to data breaches.

Toddle Compliances in China

Toddle places high importance on the privacy and security of all users' personal information, including those in China. Toddle is committed to complying with Chinese cybersecurity regulations, such as the Personal Information Protection Law (PIPL) and the Provisions on the Cyber Protection of Children's Personal Information. Toddle's toddleapp.cn domain holds ICP registration **京ICP备2021009027号-15**.

In China, Toddle operates through partnerships with CloudX Technologies Inc. and Beijing Language Partner Information Consulting Co. Ltd., with the web application hosted on web.toddleapp.cn. Backend operations are managed through AWS China (Beijing) with MLPS certification, ensuring full compliance with Chinese data protection laws. For more details on AWS China's compliance, please refer to their documentation.

Toddle has App records for its mobile applications which are as follows:

Toddle Student: **京ICP备2021009027号-20A**,

Toddle Family: **京ICP备2021009027号-21A**

Toddle Educator: **京ICP备2021009027号-22A**

Additionally, Toddle has also acquired copyright certificates from the **National Copyright Administration of the People's Republic of China** for all of its mobile applications in accordance with the "Computer Software Protection Regulations" and the "Computer Software Copyright Registration Measures". The certificates can be found **here**.

Toddle's PIPL Compliance

Lawful and Transparent Processing

Toddle collects and processes personal information strictly in line with PIPL regulations, with its Privacy Policy outlining data practices to provide transparency.

Purpose Limitation

Toddle only uses your data for the purposes specified in its agreement with you or your institution, and for which we have obtained your explicit consent. This ensures your data is used only as intended.

Data Minimization

Toddle collects the minimum amount of personal information necessary to provide its services and fulfill its obligations. This minimizes the risk associated with storing your data.

Data Security & Localization

Toddle employs industry-leading security measures to protect your data, including encryption at rest and in transit, regular security audits, and comprehensive employee training. Your data is stored securely within China on AWS Beijing servers, ensuring it remains subject to Chinese law and under your control.

Right to Information

Toddle provides transparent information about how Toddle collects, uses, and stores your personal information.

Right of Access

You can easily request access to your personal data and receive a copy in a machine-readable format by contacting Toddle at privacy@toddleapp.com.

Right to Rectification

If you find any inaccuracies in your data, you can request corrections, and Toddle will promptly update your information.

Right to Erasure ("Right to be Forgotten")

In certain situations, you can request the deletion of your personal data, and Toddle will comply with such requests in accordance with the PIPL.

Consent

Toddle understands the importance of protecting the privacy of individuals. As a Personal Information Processor under PIPL, Toddle processes data only on the instructions of the Personal Information Controllers (typically the school/teacher). The Personal Information Controller is responsible for obtaining verifiable consent before sharing any individual's personal data with Toddle.

Toddle Team

Toddle's Personal Information Protection Officer, Anshul Chauhan, is responsible for overseeing its PIPL compliance. Toddle's employees receive regular training on data protection practices and are bound by confidentiality agreements.

toddle

Thank you for trusting us!