RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Teachers First LLC ("Service Provider") on 18th November 2023 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ◉ No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ◉ No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ◉ No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ◉ No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ◉ No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ◉ No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ◉ No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ◉ No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ◉ No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ◉ No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ◉ No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ◉ No ○

3. Vendors cannot sell student information.

   Agree: Yes ◉ No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ◉ No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ◉ No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ◉ No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ◉ No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Sahil Bhargava
Print Name

18th Nov 2023
Signature, Date

Laura Assem
Print Name (Roseville City School District)

11/29/2023
Signature, Date (Roseville City School District)

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

1. We are certified for ISO 27001, ISO 27002, ISO 27017 and ISO 27018, please see attached Appendix A. We undergo comprehensive data security and privacy assessments as part of our ISO certifications and the District can request any specific evidence by emailing at privacy@toddleapp.com.
2. Toddle platform predominantly uses TLS 1.2+ (Transport Layer Security) with strong ciphers for securing connections over the Internet.
3. We utilize a Web Application Firewall (WAF) to protect our online interfaces from various web-based threats. The WAF is configured to detect and block malicious traffic, ensuring the integrity and availability of our web applications.
4. We have automated daily vulnerability testing and penetration testing every 6 months.
5. We rigorously harden our systems in alignment with the OWASP Top 10. This approach allows us to proactively address the most critical web application security risks.

Section 1.7: Internal Security

1. Please find attached "Appendix B - Privacy Policy" of Teacher Tools Private Limited (wholly-owned parent company of Teachers First LLC and Toddle App).
2. We are certified for ISO 27001, ISO 27002, ISO 27017, ISO 27018, see attached Appendix A. We are also certified for COPPA and FERPA by iKeepSafe and are signatories of the Student Privacy Pledge.
3. All data can be uploaded directly to the Toddle platform. We follow the Principle of Least Privilege to grant access to District data and only personnel deemed essential for the operation are granted access on a need to know basis.
4. We maintain access logs and undergo external audits every 6 months to ensure compliance with industry standards for data privacy. Access logs and audit reports can be shared on request by emailing at privacy@toddleapp.com.
5. Backups are performed every 5 minutes and stored in a geographically distributed location on Amazon Web Services (AWS) servers in the United States.
6. By default we maintain backups for upto 7 years or till the user requests deletion, whichever is earlier. For Roseville City School District, all data will be purged within 90 days as required under Section 1 clause 9. We send 3 reminders to the user to backup their data before deleting it permanently. We do not maintain any hard copies or print any District data.

Section II.2: Exporting of Student-Created Content

Students and parents can request for the portfolio download from within the Toddle platform. The content will be shared in a .zip file over email.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

1. Toddle will rectify any erroneous information that is brought to its notice by the school within 7 days.
2. Toddle will only accept authorised requests for edits received from the school or District. If a pupil, parent or guardian wishes to request any edits to an erroneous record, the school or District should be requested to verify and authorise the edits on their behalf.
3. The school or District in turn can reach out to their dedicated support person from Toddle (Toddle buddy) who will assist them in verifying and correcting information.
4. The school or District can also reach out to our Data Privacy Officer at privacy@toddleapp.com to review or request any changes to PII.

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data

1. Please see attached Appendix C - Information Security Policy for guidelines about ensuring data security and privacy.
2. All Toddle employees and sub-contractors undergo extensive trainings and background checks at the time of onboarding.
3. We follow the Principle of Least Privilege to restrict access to data and only the account manager and any personnel or sub-contractors considered essential for operation are given access.
4. There is information security and data privacy training at least annually to ensure all employees remain up-to-date with the best practices and maintain the highest standards of data privacy.
5. We have a comprehensive exit policy to ensure access to any and all forms of data is revoked and deleted specifically, redactions are not acceptable as per policy.

Section II.6: Disclosure Notification

1. Please refer to attached "Appendix D - Data Breach Protocol for Toddle"
2. In the event of an unauthorized disclosure of a student's records, Toddle will promptly notify Users unless specifically directed not to provide such notification by law enforcement officials. Notification shall identify: (i) the date and nature of the unauthorized use or disclosure; (ii) the 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.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

1. Toddle partners with and is certified by iKeepSafe for compliance with FERPA.
2. Toddle operates as a School Official under the FERPA regulations and complies with these regulations as it relates to children under the age of 13.
3. All information regarding Toddle's compliance with FERPA can be found at https://www.toddleapp.com/ferpa/.

Section III.5: How Student Data is Protected:

1. We use the highest standard of encryption and anonymization techniques to ensure de-identification of PII
2. We use industry-standard AES-256 encryption.
3. All data is encrypted at rest and in-transit and hosted on AWS servers in USA.
4. We have automated daily vulnerability testing and penetration testing every 6 months
5. We are subject to regular and surprise audits by independent third-party auditors and the access to the audit report can be shared on request.
6. We are compliant with ISO 27000 series, and certified by iKeepSafe for COPPA and FERPA

Reset Form

Appendix A - ISO Certificate for Teacher Tools Private Limited
Teacher Tools Private Limited is the wholly-owned parent company of Teachers First LLC and the ISO certificates are for Toddle

CERTIFICATE CERTIFICADO SERTIFIKAT CERTIFICATE

Scan this QR code with smartphone to visit our website

Certificate of Registration

This is to certify that the Information Security Management System of

TEACHER TOOLS PRIVATE LIMITED

F-1122, AMBER BLOCK, BRIGADE LAKEFRONT APP, SEETHARAMPALYA, EPIP ZONE, NEAR SAP LABS, BANGALORE, KARNATAKA, INDIA, 560048

has been assessed independently by us and found to comply with the requirements of

(Information Security Management System)

ISO 27001:2013

for the following scope:

PROVIDING END TO END SERVICES TO SCHOOLS INCLUDING PLANNING, PORTFOLIOS, REPORT CARDS, ASSESSMENTS, ETC AND DEALING WITH ALL DATA IN ORDER TO PROVIDE THESE SERVICES. THIS INCLUDES COLLECTING, STORING, ENCRYPTING, ADEQUATELY PROTECTING ALL OF THIS WITH STRONG BUSINESS CONTINUITY, DISASTER MANAGEMENT PROTOCOLS IN PLACE

Certification Calendar:

Certificate No: INI0305880/5821

Registered on: 03.05.2021

Issued on: 03.05.2021

Expires on: 02.05.2024

1st Surveillance on/before: 02.05.2022

2nd Surveillance on/before: 02.05.2023

Executive Director

RADIANCE QUALITY CERTIFICATIONS

Regd. Office - 20-22 Wenlock Rd, Hoxton, London N1 7GU, UK

Regd. off. 20-22 Wenlock Rd, Hoxton, London N1 7GU, UK

Terms & conditions

1. Validity of this certificate is subject to the organization maintaining its system in accordance with respective management systems standards along with RQC requirements.
2. This certificate remains the properly of radiance quality certifications to whom it must be returned upon request.
3. Use of logo must be in accordance with the requirement of the UKASL accredation board (in any) failure to meet the requirement shall be held liable for actions.
4. This certificate is not final evidence of certification status, status must be verified in writing from info@ukasltd.co.uk or it can be verified online at http://ukasltd.co.uk/certified-clients/

Appendix B

Teacher Tools Private Limited	PRIVACY POLICY
Version – 1.1	Release Date –29-Aug-2023

Version Control

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	01-Sep-2022	Initial Release	Nikhil Poonawala	Misbah Jafary
1.1	29-Aug-2023	Policy Review	Nikhil Poonawala	Misbah Jafary

Definitions

“Profile”
This includes personally identifiable information that we collect when you create an account. This may include First Name, Last Name, Email, and Phone Number of the user.

“Class Journal”
This includes all the content added to the class journal.

“Academic Plans”
This includes the Programme of Inquiry, Unit Plans, Learning Experiences, Assessments, Schedule, Reflections created by the teachers using the planning elements on Toddle. The external resources added by the teacher are not included in this.

“Messages”
This includes the messages sent via Toddle – both from parents to teachers and vice- versa.

“Student Portfolio”
This includes all the content added to a specific student’s portfolio.

“Student Data”
Any data collected by Toddle that can be linked back to an individual student. This contains name, age, Email ID, name of parents, school name, and the assessment data.

“Toddle Resource Bank”
A collection of all the Academic Plans created by teachers. By default, the Academic Plans are private to the

school.

“Insights”
Toddle analyses the data collected from the teachers and students and converts them into actionable points to support teachers in teaching and learning. This set of actionable data-points is collectively referred to as Insights.

What is Toddle?

Toddle is one stop solution for educators that seamlessly integrates curriculum planning, portfolios, evidence collection, progress reports and communication. Toddle has a web end as well as a mobile end. The Toddle platform has 4 different types of users – Teachers, Students, Parents, and School Administrators. Below is a brief summary of what each type of user can use the platform for:

Teachers: Teachers use Toddle for planning (Unit Plans, Lesson Plans etc), for collecting evidence of learning, for continuous reflection, for assessment evaluation and for contributing to student portfolios.

Students: Students use Toddle to document their learning journeys, set their personalised goals, receive and self-evaluate assessments, and add work to their portfolios.

Parents: Parents are linked to individual students and can see their portfolios. Parents also get access to school calendar, school news, and school policies through the Toddle Family app. The app can also be used for communicating with teachers.

Administrators: Administrators can edit and approve all the academic plans, add, delete and edit the rights of other users from their organisation. They can also see insights for better program implementation.

Parental Consent

Schools must get verifiable parental consent for using Toddle for children below legal age (as specified by the local laws). The legal age of children in the USA is 13 years. In case 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

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).

Under this Privacy Policy, you designate Toddle as a “School Official” (School Official in FERPA refers to an agency that provides a service to schools for use and maintenance of FERPA records, is under the direct control of the school and uses PII only for authorised purposes). Toddle agrees to comply with FERPA. You can find more details on Toddle and FERPA here

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 it relates 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. We do not encourage children to share their work publicly. We continuously review and update our practices to ensure compliance with COPPA requirements. You can find more details on Toddle and COPPA here.

Compliance with GDPR

Toddle collects minimal information from you and only uses it for the purposes explicitly called out in the Privacy Policy. The data collected is stored securely using industry standards. All the details with regards to the nature of the data collected and the reason for collecting it can be found in the Privacy Policy. Toddle executes a Data Processing Agreement with all the schools in the EU/ EEA and Switzerland Regions. You can find more details on Toddle and GDPR here.

Data collected by Toddle

We only collect the data that we need for providing Toddle services. It is our honest endeavour to minimise the data that we collect about our users.

We collect information from all individuals creating an account on Toddle. This includes teachers, students, parents, other family members of students, and schools.

We also collect log data from all the visitors to our website and teachers and school administrators willingly leaving data for our marketing campaigns.

Below is a list of data that we collect from our different users and and how we refer to it:

“Profile”: This includes personally identifiable information that we collect when you create an account. This may include First Name, Last Name, EMail and Phone Number of the user.

“Class Journal”: This includes all the content added to the class journal.

“Academic Plans”: This includes the Programme of Inquiry, Unit Plans, Learning Experiences, Schedule, Reflections created by the teachers using all the planning elements as specified in the customisable templates. The external resources added by the teacher are not included in this.

“Messages”: This includes the messages sent via Toddle – both from parents to teachers and vice- versa.

“Student Portfolio”: This includes all the content added to a specific student’s portfolio – photos, videos, notes, comments etc.

“Student Data”: Any data collected by us that can be linked back to an individual student. This contains name, age, Email ID, name of parents and the school name.

“Log Data”: We collect log data such as your IP address, browser type, device type, operating system, and your mobile carrier. Additionally we also use cookies to keep you logged into your system to improve your user experience.

Your rights under the GDPR

You have certain rights if you are within the EU this includes:

- **Right to access.**This right allows you to obtain a copy of your personal data, as well as other supplementary information.
- **Right to restrict processing.**You have the right to restrict the processing of your personal data in certain circumstances.
- **Right to rectification.**You have the right to have any incomplete or inaccurate information we hold about you corrected.
- **Right to object to processing.**The right to object allows you to stop or prevent us from processing your personal data. This right exists where we are relying on a legitimate interest as the legal basis for processing your Personal Data. You also have the right to object where we are processing your Personal data for direct marketing purposes.
- **Right to erasure.**You have the right to ask us to delete or remove Personal data when the personal data is no longer necessary for the purpose which you originally collected or processed.

To exercise your rights, you can contact us at privacy@toddleapp.com

Why do we collect this data?

We use the collected data only to provide services to you as laid out in the Privacy Policy and as authorised by your school. Below are a few use cases that we have for the collected data:

- Allow users to retrieve, view and edit Academic Plans
- Allow users to access and use our various features such as Journal Content, Activities, Messages etc.
- Send notifications about activities and updates on your account
- Analyse usage information to investigate, prevent, and detect activities on our service that we believe may violate the law or applicable regulations
- Provide customer support to users
- Derive insights from usage trends to develop new features or to improve the existing ones

Where do we store the data?

- Our data is hosted on Amazon Web Services (AWS) servers.
- For our users in Europe, we store the data in servers in Ireland to ensure compliance with GDPR.
- For users in other regions, they can opt for data storage in any of the following locations:
  – Australia, Ireland, United Arab Emirates, and United States of America

What is the data NOT collected for?

- We do not allow advertising or sharing data for advertising for any data collected through Toddle

- We never display ads, share data for the purpose of displaying ads, or allow data collection by advertisers or data brokers
- We never sell data to anyone for any purposes
- We never allow profiling of our users for targeted online ads

Data Retention

Toddle will keep your data for only as long as it is required or as mandated by law or as requested by the 3rd party. Before deleting your data, Toddle will send out 3 reminders to you.

When does Toddle share data with third parties?

We use a few third-party services in order to operate and improve Toddle. All these services are contractually prohibited from using that information for any other purpose other than to provide the Toddle service. You can find a list of our third party service providers here.

In case of the sale, merger, bankruptcy, sale of assets or reorganisation of our company, we may disclose or transfer your data. We will notify you of the same and the terms of this Privacy Policy will apply to your data when transferred to the new entity.

Third Party Analytics

- In order to improve your experience with Toddle, we collect and use aggregate data about usage patterns of how you use Toddle – for example, how you interact with various features on a page, the buttons that you click, the time that you spend on a page, etc. This is done to streamline existing user experience and to provide you a better experience of using Toddle.
- We use a small number of third-party services to collect and analyse this data (such as Google Analytics, Sentry). These services are contractually obligated only to use data about your usage of Toddle to provide analytics services to us and are prohibited from sharing it or using it for other purposes. You can find details of all the third party analytics services that we use here.

Cookie Policy

We use Cookies and other similar services (such as Local Storage) to keep you logged in to Toddle, customize your Toddle experience, understand how you use Toddle, and promote Toddle to relevant teachers and schools. You can remove or disable cookies via your browser settings, in which case your experience with Toddle will not be optimal.

Abandoned accounts

We consider an account to be abandoned if it has not been accessed for over a year. We will delete an account and all content associated with such accounts. However, to prevent accidental deletion, we will notify the

teacher, the school and any other email IDs associated with the account and provide an opportunity to download the data of the abandoned account.

Viewing, editing or Porting your information

Parents are encouraged to work directly with teachers and school to make any changes in your data. If however, you need to get in touch with us, you can write to privacy@toddleapp.com and we will work with the school and do our best to make the required changes.

Teachers, administrators and parents can directly edit their information in their Toddle profiles. Schools also have a right to use any other similar service and can place a request to get all of their data. We will do our best to comply to such requests. Once the pending request is processed, the data retention and deletion policies will be followed.

Deleting Toddle Account

You have the right to "forget ability", i.e., we will remove all your information from our 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. We will notify you with email before deleting your account from our database. After receiving your request, we may still retain information for up to 365 days to provide customer support and prevent accidental deletion.

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

Data Protection Practices

We follow the latest, industry standards to protect your data. Some measures that are in place include use of highly secure, access-controlled data centres, data encryption in transit, and encryption data at rest etc.

Despite these measures, in the event of a security breach, we will notify affected account holders within the amount of time required by the local law or by Toddle's internal data breach policy, whichever is more stringent, so that you can take steps to keep your data safe.

Changes to the Privacy Policy

We may from time to time make changes to this Privacy Policy to account for changes to our practices or applicable law. If we make changes to this Privacy Policy that we believe will materially affect your rights, we will notify you by email about these changes. If you continue to use our service after you receive notice of changes to this Privacy Policy, we will assume that you have accepted these changes.

For previous versions of the Privacy Policy, please reach out to us at privacy@toddleapp.com

Contact Information

Our Data Protection Officer is Misbah Jafary. If you have any questions about this Privacy Policy, please feel free to write to us at: privacy@toddleapp.com and we will reach out to you as soon as possible.

Appendix C

Teacher Tools Private Limited	Information Security Policy
Version – 1.1	Release Date – 29-Aug-2023

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	01-Sep-2022	Initial Release	Nikhil Poonawala	Misbah Jafary
1.1	29-Aug-2023	Policy Review	Nikhil Poonawala	Misbah Jafary

1) Scope

This policy applies to Teacher Tools Private Limited, its employees, its operations as well as its group companies and subsidiaries.

2) Purpose

The purpose of this policy is to define the rules and guidelines for managing information security throughout Teacher Tools Private Limited.

3) Terms and definitions

Following is an explanation of various terms used within this document

(i) LT: Leadership Team

(ii) ISG: Information Security Group

(iii) API: Application Programming Interface – Which is a software intermediary that allows two applications to talk to each other.

(iv) Information : Meaningful Data within Teacher Tools Private Limited, belonging to them or their clients.

(v) Confidentiality: Information designated as confidential is protected to meet the entity's objectives. Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian of the

information is required to limit its access, use, and retention and restrict its disclosure to defined parties.

(vi) Processing Integrity : System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

(vii) Availability : Information and systems are available for operation and use to meet the entity's objectives. Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. It addresses whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Security : Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives. Security refers to the protection of

- information during its collection or creation, use, processing, transmission, and storage and
- systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives

Privacy : Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives. Privacy applies only to personal information. The privacy criteria are organized as follows:

- Notice and communication of objectives. The entity provides notice to data subjects about its objectives related to privacy.
- Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- Collection. The entity collects personal information to meet its objectives related to privacy.
- Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
- Access. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- Quality. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- Monitoring and enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

4) Responsibilities

The primary ownership of implementing this policy is with the Leadership Team.

ISG and department heads are responsible for communicating the policy internally and externally respectively.

5) Policy

- Teacher Tools Private Limited, system and data architecture is designed to be compliant with safety standards set by regulators.

- Teacher Tools Private Limited understands that security, confidentiality, integrity, availability and privacy of data and information are critical aspects while working with clients and business partners.

- Any data or information, including but not limited to, organizational information, data, confidential data, intellectual property, personal data or personally identifiable information (PII), is a valuable asset and must be protected from unauthorized access, sharing, disclosure, modification, loss, damage and destruction.

- Managing information security of all data and information which is created, collected, acquired, stored, retained, processed, transferred, shared, distributed by Teacher Tools Private Limited, which may belong to them or to their clients or business partners, is the key towards building trust and confidence.

- Teacher Tools Private Limited, aspires to fulfill its commitment towards ensuring information security by –

    - Conducting periodical risk assessments to identify possible risks for confidentiality, privacy, security, integrity and availability of data, information assets, information systems as well as information processing facilities,

    - Employing prudent controls, policies, standards, practices, processes and procedures to mitigate and minimize the risks,

    - Identifying all applicable compliance requirements including legal, statutory, regulatory as well as contractual obligations and ensuring timely and continual compliance of them,

    - Involving and engaging employees, non-employees, outsourced resources, independent contractors, clients, business partners, service providers in the process of information security and ensuring that everybody follows policies and contributes in their responsibilities towards effective information security,

    - Creating widespread and regular awareness amongst all stakeholders about their responsibilities towards information security,

    - Committing continual improvement through effective monitoring, measurement and analysis of information security performance,

    - Implementing effective response and reporting mechanisms for information security violations and breaches as well as by planning causal analysis and corrective actions for reducing the recurrence in future,

    - Planning effective continuity of people, services and systems for ensuring continuation, resilience and restoration of client deliveries, trust, satisfaction and confidence.

Appendix D

Data Breach Protocol for Toddle

This document serves as a general outline for Toddle's data breach policy and procedure:

Date - 13th June, 2023

Definition	Any unauthorised acquisition of any unencrypted data of Toddle users acquired and maintained by Toddle that may compromise the security, confidentiality, or integrity of personal information of any user (teacher, student, or, parents)
Personal Information	Any unencrypted information that is personally identifiable, (e.g., Name, Phone Number, Email ID) collected by Toddle for delivering its services to users
Time Frame	The breach must be reported to the affected parties through email within 72 hours of the data breach being ascertained
Recipients	The point of contact at the school that the user is affiliated to
Information on the Notice	● Contact Information of the Toddle Data Officer ● A general description of the breach incident ● An explanation, to the best of Toddle's knowledge, of what happened ● The types of personal information that are believed to be compromised ● If known, the date and time of the breach, or best an estimate ● Reasons for delay of notification (if any) ● Steps taken by Toddle to mitigate the situation and to avoid it from repeating
Mode of the Notice	Email to the school
Adherence to Local Laws	In the event of a data breach, Toddle will adhere to the applicable state data breach regulations of the impacted user(s)

Deepanshu

Deepanshu Arora
Founder and CEO, Toddle