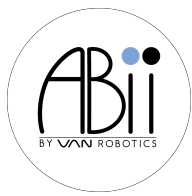


VAN ROBOTICS DATA PRIVACY POLICY

**Van Robotics Inc
712 Richland Street, Suite F
Columbia, SC 29201**

**Reviewed and Approved:
April 2022**



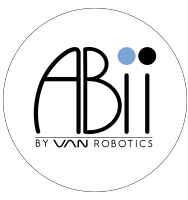
Van Robotics Student Data Privacy Pledge

Van Robotics will not:

- Collect, maintain, use or share Student Data beyond that needed for authorized educational/school purposes
- Sell Student Data to third parties
- Make material changes to School Service Provider education privacy policies without first providing prominent notice to the users and/or account holder(s) (i.e., the institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent).
- Use identifiable Student Data to market or advertise to prospective customers

Van Robotics will:

- Clearly disclose what types of Student Data we collect
- Support access to and correction of Student Data by the student or their authorized guardian or parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.
- Maintain a comprehensive security program that is reasonably designed to protect the security, confidentiality, and integrity of Student Data against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.
- Provide resources to support educational institutions/agencies, teachers, or parents/students to protect the security and privacy of Student Data while using Van Robotics' products or services.
- Allow a successor entity to maintain the Student Data, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected Student Data.
- Incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws.
- Require that all Van Robotics' employees with access to Student Data sign a confidentiality agreement upholding the systems and policies consistent with the Van Robotics DPP.



❖ POLICY AND SCOPE OF DATA COLLECTION

Data Privacy Policy (DPP). The purpose of this DPP is to describe the systems and policies in place at Van Robotics to protect data collected and/or stored through the use of its products and services. These systems and policies include, but are not limited to, compliance with all applicable federal and state guidelines and statutes defined in FERPA, CIPA, and COPPA.

Van's Products and Services. Van Robotics provides the following digital educational products and services described below:

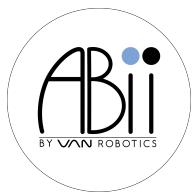
- AI-enabled robots, named ABii, which include national and state standards-aligned math, reading and social-emotional learning lessons
- Class-level and student reports to evaluate performance and attention improvements
- Software subscription for the Lesson Creation Tool (available in English, Spanish, Mandarin, German and Hindi)
- Professional Development to support ABii set up, classroom integration and best practices
- Professional Development to support use of the Lesson Creation Tool

Student Data to be Provided, Collected and/or Stored. Users of the ABii robot will provide student names and grade levels in order to record and adapt to individual student performance and attention. The ABii robot will collect information about each student's performance and attentional targets during each lesson. **No video, images or audio data is recorded or stored by the robot.** Reports will be automatically generated and made available to teachers and administrators to reflect individual student and class progress. Further, reports regarding ABii robot usage by teachers and students will be made available to the Local Education Agency's (LEA's) administrators.

❖ DATA OWNERSHIP

All Student Data collected and stored by Van Robotics will continue to be the property of and under the control of the LEA. Van Robotics will ensure that all copies of Student Data collected by or for products and services maintained by Van Robotics, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this privacy policy in the same manner as the original Student Data. Van Robotics may destroy and/or transfer student content collected by its products to a separate account, according to the procedures set forth below.

Requests for Student Data. In the event that a member of the Van Robotics team receives a request from a parent, authorized guardian or a third party to alter or destroy their own Student's data from one of Van Robotics products or services, Van Robotics will refer the requestor to the LEA and forward the original request to the LEA.



Data Transfer. Upon written request from the LEA, the transfer of Student Data will be initiated by Van Robotics and will include (1) transferring identifiable Student Data to a digital format and (2) sharing the digital copy of the Student Data with the requesting LEA.

Data Destruction. Upon written request from the LEA, the destruction of Student Data will be initiated by Van Robotics and will include (1) shredding hard copies of student data; (2) deleting digital copies of student data or otherwise de-identifying Student Data, or rendering it unreadable or indecipherable by human or digital means. Upon completion, Van Robotics will provide written notification to LEA.

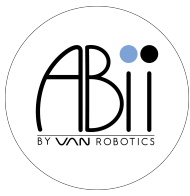
❖ DATA PROTECTION

Data Security. Van Robotics will maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. These measures include:

- **Passwords and Employee Access.** Access to Van Robotics' products, services and Student Data will be protected with secure usernames and passwords, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Access to Student Data will be limited to employees or contractors who are directly involved with supporting Van Robotics products and services used by the LEA. Further, any employee with access to Student Data will be required to sign confidentiality agreements regarding Student Data.
- **Security Protocols.** Van Robotics will maintain all Student Data in a secure digital environment to ensure that data may only be viewed or accessed by parties legally allowed to do so. Van Robotics uses secure transfer protocols to transfer data between Van Robotics' products and services, and data is encrypted at rest in cloud storage devices protected by appropriate firewalls. When Van Robotics' products and services are accessed using a supported web browser, Van Robotics employs industry standard measures to protect data from unauthorized access, including server authentication and data encryption.
- **Periodic Risk Assessment.** Van Robotics will conduct periodic digital risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Van Robotics will notify the LEA within a reasonable amount of time of the incident. As part of that notification process, Van Robotics will initiate the following procedure:

1. The designated contact at the LEA will be sent an email with the subject "Notice of Data Breach" and,



2. A description of the security breach will be provided, including but not limited to the following: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.”
 - Van Robotics agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - At the request of the LEA, Van Robotics will assist in providing notice of unauthorized access to affected parents, legal guardians or eligible pupils of the unauthorized access, which shall include the information listed in the data breach procedure described above.
 - In the event of a breach originating from LEA’s use of the Service, the Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.