

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Liverpool Central School District

and

Arduino S.r.l.

This Data Privacy Agreement ("DPA") is by and between the Liverpool Central School District ("EA"), an Educational Agency, and Arduino S.r.l. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 2/5/2021 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New

York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII

shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities)

whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Daniel Farsaci

Title: Director of Technology

Address: 190 Blackberry Road

City, State, Zip: Liverpool, NY 13090

Email: dfarsaci@liverpool.k12.ny.us

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its’ Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA’s notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.



EDUCATIONAL AGENCY	CONTRACTOR
BY: [Signature] 	BY: 
[Printed Name] Daniel Farsaci	Francesco Fabio Domenico Violante
[Title] Director of Technology	Chairman of the Board of Directors
Date: 6/16/21	Date: 06 / 15 / 2021

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children’s Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: dfarsaci@liverpool.k12.ny.us. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.


CONTRACTOR	
[Signature]	
[Printed Name]	Francesco Fabio Domenico Violante
[Title]	Chairman of the Board of Directors
Date:	06 / 15 / 2021

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Arduino Srl
Description of the purpose(s) for which Contractor will receive/access PII	See attached DSPP
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR Data</p>
Contract Term	<p>Contract Start Date _____</p> <p>Contract End Date _____</p>
Subcontractor Written Agreement Requirement	<p>Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)</p> <p><input checked="" type="checkbox"/> Contractor will not utilize subcontractors.</p> <p><input type="checkbox"/> Contractor will utilize subcontractors.</p>
Data Transition and Secure Destruction	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>See attached DSPP</p>
Encryption	Data will be encrypted while in motion and at rest.


CONTRACTOR	
[Signature]	
[Printed Name]	Francesco Fabio Domenico Violante
[Title]	Chairman of the Board of Directors
Date:	06 / 15 / 2021

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

[remainder of page intentionally left blank]



Data Security and Privacy Plan (DSPP)

Table of contents

I. Objective and Scope	3
A. Relationship Between Security and Privacy	3
B. Shared Responsibility	3
C. Defining the Purpose	4
D. Allowed and Prohibited Access/Use/Disclosure	4
E. State/Local Data Privacy Regulations	4
F. Standard Student Data Privacy Practices	5
1. Restrictions on Use and Release of Student Information	5
2. Parents' Right to access and review	5
3. Reasonable Safeguards to Protect Confidentiality	5
4. Addressing Privacy Concerns, Rights and Complaints	5
III. Protection of Personally Identifiable Student Information	6
A. Security Strategy	6
B. Organizational Controls	6
C. Infrastructure	6
E. Secure Software Development Practices	7
F. Logical Access Control	7
G. System monitoring and testing	7
IV. Breach notification requirements	8
V. Data Retention and Disposal	8



I. Objective and Scope

In providing Arduino Education Solutions, Arduino acknowledges that it has a serious obligation to protect the confidentiality of student data processed for the use of related cloud services provided.

As a technology contractor for your District, we recognize that we share certain responsibilities to protect the security and privacy of sensitive data that is processed by our systems. This Data Security and Privacy Plan (DSPP) outlines the administrative, technical and physical safeguards used to meet these responsibilities.

Arduino does not process and store educational data but could process personally identifiable information (PII) of students using Arduino Education Solutions, in particular Arduino Cloud services. In any event, Arduino does not process personal data of children under the age of 14 and, in case of students under the age of 14 using Arduino Education solutions, those will not be identified, as unique and anonymous access credentials are given only and directly to the teacher.

With regard to the processing of personal data of students, including minors, please read Arduino Privacy Policy at <https://www.arduino.cc/en/privacy-policy> with specific reference to minors at <https://www.arduino.cc/en/privacy-policy#minors>

Arduino acknowledges that PII are protected under EU GDPR Regulation, FERPA, PPRA, COPPA and other federal, state and local regulations, including NY State Education Law section 2-d and California's SOPIPA.

Arduino's Privacy Policy strictly prohibits the sale of users, including student and community data under any circumstances, or the unauthorized sharing of that data with other parties. Data collected is only used for the approved purposes and in accordance with Arduino's Privacy Policy.

II. Data Security and Privacy Obligations

A. Relationship Between Security and Privacy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support best practices and policies.

B. Shared Responsibility

Privacy regulations define several distinct roles with respect to data:

- Data subject/owner: the individual, natural person, who is identifiable or identified student, staff, parent;
- Data controller: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- Data processor: natural or legal person, public authority, agency or other body which processes, including but not limited as provider of technology/services, personal data on behalf of the controller for the determined purposes.

Please note that Arduino processes PII in relation to Arduino Educational Solutions as autonomous data controller and does not process PII as data processor on behalf of District hence, there is direct relationship between Arduino or District and the data subject/owner.

Arduino and the District, each as autonomous data controller, have the primary responsibility for ensuring



that data they controlled and processes are protected appropriately throughout all phases of life cycle.

Arduino's role is to:

- define their business needs or purpose for collecting data
- designate personnel responsible for data privacy matters
- establish privacy policies and practices aligned with the defined purpose
- communicate directly with students/teacher/parents regarding data collection and use
- obtain consent for data collection as appropriate
- define the conditions under which the data is no longer needed and should be purged (data retention/disposal policy)
- provide awareness training to ensure that its staff, administrators, and volunteers know how to handle sensitive data properly
- communicate privacy objectives to internal users and contractors
- provide the technical means to process data securely
- protect data while it is in custody
- securely remove data when it is no longer needed

Note that Arduino does not process PII and interact directly with the data subjects for PII that falls under District control.

C. Defining the Purpose

Arduino's Privacy Policy and applicable Cloud services license limit the "purpose" of Arduino data processing to the creation of student Arduino Account and provide the Arduino services requested.

In particular Arduino services are essentially providing two major functionalities to student users:

- online editing of a sketch (Online Editor or Create Editor)
- IoTCloud - data collection from IoTDevices and capabilities to create dashboards to visualize data (for example temperature coming from a sensor) or control remote devices (for example switch on a light)

D. Allowed and Prohibited Access/Use/Disclosure

Student data, whether provided to Arduino by data subject or generated by Arduino through normal system operation, is only to be used for the above defined purposes. Within Arduino, data is only shared with employees who have a legitimate need to access it in connection with the data subject requested services. All employees, whether or not they have access, receive security and privacy awareness training.

Data exchange handled using a secure API and plugin (developed and provided by Arduino). Installation of and access to the plugin is managed by Arduino. Once the plugin is installed and enabled, a unique Client ID is generated specifically for the plugin delivered via the plugin registration process.

Arduino will not disclose any personally identifiable information to any other party without prior written consent of the data subject, unless required by statute or court order.

E. State/Local Data Privacy Regulations

Arduino acknowledges that in accordance with NY State Education Law section 2-d, each district must publish a Parents' Bill of Rights (PBOR), which outlines the District's specific student data privacy responsibilities and expectations.



Arduino is also in compliance with EU GDPR Regulation, federal and California privacy law requirements, including FERPA, COPPA, PPRA, and the Student Online Personal Information Protection Act (SOPIPA).

Specific requirements are set forth with respect to adequate data protection measures, data breach notification procedures, etc. Other state and federal regulations outline similar requirements. Arduino stays continuously updated on evolving privacy regulations and will work to be in compliance with those.

F. Standard Student Data Privacy Practices

1. Restrictions on Use and Release of Student Information

Student data, whether provided to Arduino by data subject or generated by Arduino through normal system operation, is only to be used for the purposes of providing Arduino services to and requested by students/data subjects.

In accordance with applicable data privacy laws and Arduino's Privacy Policy, Arduino will not sell a student personally identifiable information or release it for any commercial purpose.

Within Arduino, access to student and community data is only granted to individuals who need such access to perform their job functions in connection with the services provide. Arduino's employees are prohibited from accessing this data for any other purpose, and are made aware of this restriction through policy, specific instructions and training.

In order to provide the services requested by data subject, it may be necessary to share student information with subcontractors. Arduino maintains a third-party risk management program to ensure that such subcontractors abide by applicable data protection and security requirements.

2. Parents' Right to access and review

Arduino acknowledges that parents have the right to inspect and review the complete contents of their child's record. It is Arduino's responsibility to provide parents with access to this information as defined in its Privacy Policy and in accordance with the procedure and rights set forth therein. Arduino will provide technical assistance as appropriate.

3. Reasonable Safeguards to Protect Confidentiality

Arduino acknowledges its responsibility to protect the confidentiality of personally identifiable information in custody, throughout its entire lifecycle, using reasonable administrative, technical and physical safeguards associated with industry standards and best practices. Specific protection measures in use are described in Section III of this document.

4. Addressing Privacy Concerns, Rights and Complaints

Arduino acknowledges that parents have the right to have complaints about possible breaches of student data addressed. Complaints can be directed as defined in Arduino's Privacy Policy as well exercise of rights granted and information about the data processors and the persons authorized by the data controllers to process data should be directed to privacy@arduino.cc.

Arduino Data Protection Officer is also available for addressing data protection issues and concerns. In addition to the privacy@arduino.cc any concerns about Arduino's privacy practices and data protection can be directed to dpo@arduino.cc.

III. Protection of Personally Identifiable Student Information

A. Security Strategy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls.

We ensure data security using a combination of Preventive, Detective, and Organizational controls, including network architecture and configuration, software design, policies, procedures and other critical protective measures.

Because there is never a guarantee of full prevention, our program also includes Response and Recovery controls.

B. Organizational Controls

Policies are distributed to new employees as part of onboarding, reviewed throughout the year as part of ongoing risk assessment and updated according to business/technology changes when appropriate.

Updated versions are published at least annually and distributed to employees for acknowledgement.

C. Infrastructure

Data protection starts with a secure infrastructure based on Cloud providers (Amazon Web Services and Google Compute Platform) and third party services also hosted in Cloud.

For a complete list of providers used see <https://www.arduino.cc/en/Main/PrivacyPolicy>

The Authentication phase plays a major role of the security protection, and Arduino is utilizing a service that provides:

- Web protection against several common threats to web applications such as XSS (cross-site scripting), Clickjacking or Cross-site request forgery.
- Anomaly Detection such as Brute-Force Protection: provides protection against suspicious failed login attempts.
- Universal Login Support: increase security so that users have the ability to use their social logins without the need of sharing their credentials with us.
- Security Rules: to enforce access to control so that only Arduino employees can access selected resources

Another fundamental component of our protection strategy from infrastructure standpoint is our content delivery network, that provides:

- DDoS protection: mitigation of denial-of-service attacks to ensure that services are not affected by a high number of malicious requests;
- Firewalling: protection against the most common web applications attacks

Sensitive data that requires special handling falls into several categories:

- PII of students (if Arduino users) - username, password, name, surname, email address, user profile picture and home address (for shipment and billing)
- PII of teachers (if Arduino users)

Data encryption is applied to our databases containing PII:

- Protection at rest:

- PII are stored in Databases using DB-level encryption based on AES-256
- Protection in transit:
 - any Browser-based or API-based communication uses HTTPS protocol secured with TLS
 - IoT devices are sending data to cloud using MQTT protocol secured with TLS

E. Secure Software Development Practices

Application code vulnerabilities can result in direct or indirect exposure of sensitive information. In order to prevent this, Arduino applications are developed and tested in accordance with industry-recognized best practices.

- Developers have specific know how and receive training on secure architectural and coding standards
- Separate Development/Test/Production environments to avoid the risk of introducing security flaws into live systems, and minimize exposure of sensitive data during development lifecycle
- Change control processes ensure that new code is reviewed, tested and approved before being released
- Dedicated expert Cybersecurity Engineers are responsible for reviewing architectures and code changes in order to spot vulnerabilities and design flaws and apply proper remediations

F. Logical Access Control

Logical access control is governed by the principle of least privilege. Specific users are granted the minimum access needed to perform their job functions.

In general, most Arduino internal staff members do not have direct access to PII or Arduino's services users, with the following exceptions:

- Our customer support team has administrator-level access to assist users with technical issues.
- Only specific members of technical staff can access the databases directly, by remotely connecting to servers via the VPN. VPN access is only granted to those members who need it to perform their job functions, and is limited to specific network segments based on role. Multi-factor authentication is used during the VPN authentication process. The access control list is reviewed periodically to determine whether access is still needed. Accounts are modified or disabled based upon changes in job responsibilities.
- Non-development staff will be granted privileges on an as-needed basis. Access requirements must be documented and approved by management before access is granted.

All Arduino's employees (including contractors and vendors with access to Arduino systems) are responsible for taking appropriate steps to select and secure their passwords, including the use of a Password Management service which allows generation of secure passwords. On-boarding and periodic security awareness training and policies outlines current "best practice" recommendations for managing passwords.

G. System monitoring and testing

Arduino continuously monitors its systems for unauthorized activity that may result in the exposure of sensitive data.



Monitoring tools in use are capable of collecting and concentrating application logs for analysis, and are applying automated anomaly detection to identify for example brute force attacks.

Arduino's Security Team is conducting:

- Application log reviews - application logs are centralized using log analytics tools to allow analysis for detection of external threats
- Vulnerability assessment and penetration testing of Cloud services - results are reviewed by Security Engineers and any issues are remediated in a timely manner to reduce the potential for exploit of system vulnerabilities from the outside

IV. Breach notification requirements

Should Arduino become aware of any unauthorized release of student data, in violation of applicable privacy laws and/or binding contractual obligations relating to data privacy and security, we will notify the designated privacy Authority in the most expedient way possible and without unreasonable delay.

Should an Arduino user or customer suspect a vulnerability or security issue, they are invited to report it as described in our Coordinated Vulnerability Disclosure policy available at <https://www.arduino.cc/en/security>

If there is valid reason to suspect a breach (i.e., clients report fraudulent activity on their accounts, or we see signs that someone has gained unauthorized remote or physical access to the data center), Arduino incident response team will: check for common indicators of compromise to determine whether or not a breach has actually occurred.

- Notify CIO, security team, and application owners of findings.
- Conduct additional research as necessary to determine the extent of impact.

If it is determined that a breach has occurred, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.) An official statement will be issued, summarizing our findings and providing an estimated time frame for service restoration.

V. Data Retention and Disposal

PII data will only be stored as long as the Arduino legitimately needs it and in accordance with Arduino's Privacy Policy.

TITOLO	Liverpool Central School District - Ed-law 2-D Rider (DPA)
NOME FILE	Arduino_Execution.docx and 1 other
ID DOCUMENTO	642fdec4e7d7d4b3f951038e1dde11b1cdece8f0
FORMATO DATA AUDIT TRAIL	MM / DD / YYYY
STATO	● Completati

Cronologia documento



06 / 15 / 2021
15:29:35 UTC+2

Inviato per la firma a Francesco Fabio Domenico Violante
(f.violante@arduino.cc) da g.maesa@arduino.cc
IP: 2.233.88.140



VISUALIZZATO

06 / 15 / 2021
16:46:37 UTC+2

Visualizzato da Francesco Fabio Domenico Violante
(f.violante@arduino.cc)
IP: 93.65.57.235



FIRMATO

06 / 15 / 2021
16:46:48 UTC+2

Firmato da Francesco Fabio Domenico Violante
(f.violante@arduino.cc)
IP: 93.65.57.235



COMPLETATO

06 / 15 / 2021
16:46:48 UTC+2

Il documento è stato completato.