

# DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the “Agreement”) is made and entered into by and between EDpuzzle, Inc. (the “Vendor”) and Bolivar-Richburg Central School District.

**WHEREAS**, Bolivar-Richburg Central School District and Vendor are parties to a contract or other written agreement (Vendor’s Terms of Service and Privacy Policy, available at [www.edpuzzle.com/terms](http://www.edpuzzle.com/terms) and [www.edpuzzle.com/privacy](http://www.edpuzzle.com/privacy) respectively, both hereinafter referred as the “Contract”) pursuant to which the Vendor will receive student data and/or teacher or principal data (“Protected Data”) that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from Bolivar-Richburg Central School District for purposes of providing certain products or services to Bolivar-Richburg Central School District; and

**WHEREAS**, both Bolivar-Richburg Central School District and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

**NOW THEREFORE**, in consideration of the mutual promises and covenants contained in the Contract, as well as in this Agreement, the parties hereto mutually agree as follows:

## 1. **Confidentiality**

- a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided for in the Agreement is deemed confidential information.
- b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with federal and state law and that any information obtained will not be revealed to any persons, firms or organizations, except as otherwise provided in this Agreement or the Contract.

## 2. **Data Protections and Internal Controls**

- a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by Bolivar-Richburg Central School District that directly relate to a student(s) (hereinafter referred to as “education record”).
- b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:

1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and
2. Not use the education records for any other purpose than those explicitly authorized in the Contract and/or Agreement; and
3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and
4. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

**3. Data Security and Privacy Plan**

- a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from Bolivar-Richburg Central School District.
- b. Vendor understands and agrees that it is responsible for submitting a Data Security and Privacy Plan to Bolivar-Richburg Central School District prior to the start of the term of the Agreement, and it shall:
  1. Outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with Bolivar-Richburg Central School District's policy on data security and privacy, as adopted.
  2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from Bolivar-Richburg Central School District under the Contract.
  3. Outline the training requirement established by the Vendor for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

**4. Notice of Breach and Unauthorized Release**

- a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:
  1. Immediately notify Bolivar-Richburg Central School District in the most expedient way possible and without unreasonable delay, **but no more than seven (7) calendar** days after Vendor has discovered or been informed of the breach or authorized release.
  2. Advise Bolivar-Richburg Central School District as to the nature of the breach

and steps Vendor has taken to minimize said breach.

- b. In the case of required notification to a parent or eligible student, the Vendor shall:
  1. Promptly reimburse Bolivar-Richburg Central School District for the full costs of such notification.
- c. Vendor will cooperate with Bolivar-Richburg Central School District and provide as much information as possible directly to Bolivar-Richburg Central School District about the incident, including but not limited to:
  1. The description of the incident;
  2. The date of the incident;
  3. The date Vendor discovered or was informed of the incident;
  4. A description of the types of Protected Data involved;
  5. An estimate of the number of records affected;
  6. The schools within Bolivar-Richburg Central School District affected;
  7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data; and
  8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- d. The Vendor shall indemnify and hold Bolivar-Richburg Central School District harmless from any claims arising from its breach within the Data Sharing and Confidentiality Agreement confidentiality and data security and privacy standards provision.
- e. Vendor acknowledges that upon initial notification from Vendor, Bolivar-Richburg Central School District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (“CPO”). Vendor agrees not to provide this notification to the CPO directly unless requested by Bolivar-Richburg Central School District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Bolivar-Richburg Central School District, Vendor will promptly inform Bolivar-Richburg Central School District of the same.

## **5. Vendor Information**

Vendor understands that as part of Bolivar-Richburg Central School District’s obligations

under New York Education Law Section 2-d, Vendor is responsible for providing Bolivar-Richburg Central School District with Vendor information (see Vendor Information for Data Privacy and Security) to include:

- a. Exclusive purposes for which the student data will be used;
- b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;
- c. Whether student data will be returned or destroyed upon expiration of the Agreement;
- d. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and
- e. Where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

**6. Termination or Expiration of Contract and/or Agreement**

- a. Upon termination of the Agreement and written request by Bolivar-Richburg Central School District, Vendor shall destroy all confidential information obtained in connection with the services provided therein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement.
- b. If requested by Bolivar-Richburg Central School District, Vendor will assist Bolivar-Richburg Central School District in exporting Student Gradebooks<sup>1</sup> previously received back to Bolivar-Richburg Central School District for its own use, prior to deletion, in a standard exportation format.
- c. In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate, upon written request by Bolivar-Richburg Central School District, with Bolivar-Richburg Central School District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- d. Vendor may use De-identified data for purposes of research, improvement of Vendor's product or services, and/or development of new products and services. In

---

<sup>1</sup> Names, responses, grades and results obtained by students in their assignments.

no event shall Vendor or any of its subcontractors or assignees re-identify or try to re-identify any De-identified data or use De-identified data in combination with other data elements possessed by Vendor or any third-party affiliate, posing risk of re-identification.

- e. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data on any storage medium whatsoever, except for data backups that are part of Vendor's disaster recovery storage system, which may be retained for an additional term of thirteen (13) months after termination of the Agreement, provided such backups remain inaccessible to the public and are unable to be used by the Vendor in the normal course of its business. Upon request, Vendor will provide Bolivar-Richburg Central School District with a certification from an appropriate officer that these requirements have been satisfied in full.

# PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Bolivar-Richburg Central School District seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our district and school operations.

The Bolivar-Richburg Central School District seeks to insure that parents have information about how the District stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Bolivar-Richburg Central School District has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 7240, Student Records: Access and Challenge. You may access this Policy from the District's website.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to **Bolivar-Richburg Central School District-Data Privacy Officer, 100 School Street, Bolivar, New York 14715** or by using the form found at the schools Technology webpage, or directly at: <https://www.brcs.wnyric.org/Page/4065>. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>

Supplemental Information About Third Party Contracts

In order to meet 21<sup>st</sup> century expectations for effective education and efficient operation, the District utilizes several products and services that involve third party contractors receiving access to student data, or principal or teacher data, protected by Section 2-d of the Education Law. The District recognizes that students, parents, and the school community have a legitimate interest in understanding which of the District's vendors receive that data, for what purpose, and under what conditions. The District has undertaken the task of compiling that information, and of insuring that each new contract adequately describes (1) the exclusive purposes for which the data will be used, (2) how the contractor will ensure that any subcontractors it uses will abide by the data protection and security requirements, (3) when the contract expires and what happens to the data at that time, (4) if and how an affected party can challenge the accuracy of the data is collected, (5) where the data will be stored, and (6) the security protections taken to ensure the data will be protected, including whether the data will be encrypted.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year of the last signature affixed.

*Julia Trius*

\_\_\_\_\_  
Authorized Vendor Signature

03 / 09 / 2021

\_\_\_\_\_  
Date

*Dan Davison Jr.*

\_\_\_\_\_  
Authorized Bolivar-Richburg Central School District  
Signature

2/25/2021

\_\_\_\_\_  
Date

## VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: EDpuzzle Inc.	Product: The Edpuzzle Instructional Software, accessible at <a href="http://www.edpuzzle.com">www.edpuzzle.com</a>
Collects: <input checked="" type="checkbox"/> Student Data <input checked="" type="checkbox"/> Teacher or Principal Data <input type="checkbox"/> Does not collect either	

Educational agencies including Bolivar Richburg Central School are required to *post information about [third-party contracts](#) on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to [NYS Education Law 2-d](#) and [Part 121.3 of the Commissioner's Regulations](#). Note that this applies to all software applications and to mobile applications (“apps”).

### Part 1: Exclusive Purposes for Data Use

The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:

Student and Teacher Data will be used by third-party contractor for improving the Services and for the following limited purposes:

- a) to create the necessary accounts to use the Service;
- b) to provide teachers with analytics on student progress;
- c) to send teachers email updates, if applicable;
- d) to help teachers connect with other teachers from the same school or district;
- e) to assess the quality of the Service;
- f) to secure and safeguard personal information of other data subjects;
- g) to comply with all applicable laws on the protection of personal information.

### Part 2: Subcontractor Oversight Details – Select the appropriate option below.

This contract has no subcontractors.

This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey data protection and security requirements consistent with those that the third-party contractor is required to obey under state and federal law:

Third-party contractor shall assess the privacy and security policies and practices of the assignees, agents or subcontractors to ensure such third-party service providers comply with best industry standards, including, but not limited to, ISO and NIST regulations.

### Part 3: Contract Lifecycle Practices

The contract expires in accordance with the terms outlined in the attached Data Privacy and Security Plan, unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires and upon request by Bolivar-Richburg Central School District, protected data will be deleted by the contractor, via shredding, returning of data, mass deletion. Upon request, Student Gradebooks may be exported for use by Bolivar-Richburg Central School District before deletion.

### Part 4: Student Educational Records / Improper Disclosure



A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the [U.S. Department of Education FERPA website](#).

B. A complaint or report of improper disclosure may be completed by submitting the [Improper Disclosure Report](#) form.

**Part 5: Security Practices**

A. Protected data provided to the contractor will be stored: (include *where* and *how*)

The data is stored in externalized databases that are currently being provided by MongoDB Atlas (security and compliance information accessible at <https://www.mongodb.com/cloud/trust>), and simultaneously hosted on Amazon Web Services (security and compliance information accessible at <https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html>) in North Virginia (United States).

B. The security protections taken to ensure data will be protected that align with the [NIST Cybersecurity Framework](#) and industry best practices include, but are not limited to:

- Pseudonymisation and encryption of PII (TLS v1.2 for all data in transit between clients and server and AES256-CBC (256-bit Advanced Encryption Standard in Cipher Block Chaining mode) for encrypting data at rest).
- Password protection.
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Restore the availability and access to personal data in a timely manner in the event of a technical incident.
- Regularly test, assess and evaluate the effectiveness of technical and organizational measures ensuring the security of the processing.

**Part 6: Encryption Practices**

■ By checking this box, contractor certifies that data encryption is applied in accordance with [NYS Education Law Section 2-d 5\(f\)\(5\)](#).



EDpuzzle, Inc.  
833 Market St. (Suite 427)  
San Francisco, CA 94103  
privacy@edpuzzle.com

## DATA PRIVACY AND SECURITY PLAN FOR EDPUZZLE AND SUPPLEMENTAL INFORMATION

The technical and organizational measures provided in this Data Privacy and Security Plan and Supplemental Information (hereinafter, “DPSP”) apply to EDpuzzle, Inc. (hereinafter, “Edpuzzle”) in the processing of Personally Identifiable Information (“PII”) that is the subject matter of the Agreement entered into with Bolivar-Richburg Central School District (“District”) (the “Agreement”), including any underlying applications, platforms, and infrastructure components operated and managed by Edpuzzle in providing its services.

### 1. COMPLIANCE WITH THE LAW

Edpuzzle hereby commits to fully comply with all applicable federal and state laws and regulations on data protection that apply to the processing of PII that is the subject matter of the Agreement. Such laws and regulations may include, without limitation:

- (a) New York State Education Law §2-D.
- (b) Family Educational Rights and Privacy Act of 1974 (“FERPA”).
- (c) Children’s Online Privacy Protection Act (“COPPA”).
- (d) Children’s Internet Protection Act (“CIPA”).
- (e) Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), if applicable.

### 2. DATA PROTECTION

2.1. Student and Teacher Data will be used by Edpuzzle for improving the Services and for the following limited purposes:

- a) to create the necessary accounts to use the Service;
- b) to provide teachers with analytics on student progress;
- c) to send teachers email updates, if applicable;
- d) to help teachers connect with other teachers from the same school or district;
- e) to assess the quality of the Service;
- f) to secure and safeguard personal information of other data subjects;
- g) to comply with all applicable laws on the protection of personal information.

Edpuzzle shall not use PII for any purposes other than those authorized pursuant to the Agreement and may not use PII for any targeted advertising or other commercial uses. Nevertheless, teachers utilizing the Edpuzzle service may provide express consent to receive marketing or commercial communications from Edpuzzle.

2.2. Edpuzzle shall keep strictly confidential all PII that it processes on behalf of District. Edpuzzle shall ensure that any person that it authorizes to process the PII (including Edpuzzle's staff, agents or subcontractors) (each an "authorized person") shall be subject to a strict duty of confidentiality. Edpuzzle shall ensure that only authorized persons will have access to, and process, PII, and that such access and processing shall be limited to the extent strictly necessary to provide the contracted services.

2.3. During their tenure, all employees are required to complete a refresh of privacy and security training at least annually. They are also required to acknowledge that they have read and will follow Edpuzzle's information security policies at least annually. Some employees, such as engineers, operators and support personnel who may have elevated access to systems or data, will receive additional job-specific training on privacy and security. Edpuzzle may also test employees to ensure they have fully understood security policies. Employees are required to report security and privacy issues to appropriate internal teams in accordance with Edpuzzle's Incident Response Plan ("IRP"). Employees are informed that failure to comply with acknowledged policies may result in consequences, up to and including termination of employment agreements.

2.4. Edpuzzle shall not retain any personal data upon completion of the contracted services unless a student, parent or legal guardian of a student may choose to independently establish or maintain an electronic account with Edpuzzle after the expiration of the Agreement for the purpose of storing student-generated content.

2.5. 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, users may access, correct, update, or delete personal information in their profile by signing into Edpuzzle, accessing their Edpuzzle account, and making the appropriate changes.

### 3. DATA SECURITY

3.1. Edpuzzle shall implement and maintain reasonable and appropriate technical and organizational security measures to protect the PII with respect to data storage, privacy, from unauthorized access, alteration, disclosure, loss or destruction. Such measures include, but are not limited to:

- Pseudonymisation and encryption of PII (TLS v1.2 for all data in transit between clients and server and AES256-CBC (256-bit Advanced Encryption Standard in Cipher Block Chaining mode) for encrypting data at rest).
- Password protection.
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Restore the availability and access to personal data in a timely manner in the event of a technical incident.
- Regularly test, assess and evaluate the effectiveness of technical and organizational measures ensuring the security of the processing.

3.2. In the event that PII is no longer needed for the specific purpose for which it was provided, it shall be destroyed as per best practices for data destruction using commercially reasonable care, security procedures and practices.

3.3. Upon the discovery by Edpuzzle of a breach of security that results in the unauthorized release, disclosure, or acquisition of student data, or the suspicion that such a breach may have occurred, Edpuzzle shall:

- (a) promptly notify District of such incident. Edpuzzle will provide District with reasonably requested information about such security breach and status of any remediation and restoration activities; and
- (b) Complaints on how breaches of Student Data are addressed shall be made to Edpuzzle's Data Protection Officer at Av. Pau Casals 16, Ppal. 2-B, 08021 Barcelona, Spain or at [privacy@edpuzzle.com](mailto:privacy@edpuzzle.com), as foreseen in Edpuzzle's Privacy Policy.

#### 4. COOPERATION AND INDIVIDUALS' RIGHTS

4.1. To the extent permitted by applicable laws, Edpuzzle shall provide reasonable and timely assistance to District to enable District to respond to:

- (1) any request from an individual to exercise any of its rights under applicable data protection laws and regulations; and
- (2) any other correspondence, enquiry or complaint received from an individual, regulator, court or other third party in connection with the processing of Student Data.

4.2. In the event that any such communications are made directly to Edpuzzle, Edpuzzle shall instruct such individual to contact the District directly.

4.3. Parents and legal guardians shall have the right to inspect and review the complete contents of his or her child's processed personal data. Parents and legal guardians that request copies of their children's personal information shall contact District's personnel to that end. At any time, District can refuse to permit Edpuzzle to further collect personal information from its students, and can request deletion of the collected personal information by contacting Edpuzzle at [privacy@edpuzzle.com](mailto:privacy@edpuzzle.com).

#### 5. THIRD-PARTY SERVICE PROVIDERS

5.1. To the extent permitted by law, and as reasonably necessary to provide the Edpuzzle Service to the District, Edpuzzle may provide access to, export, transfer, or otherwise disclose student and/or teacher data to Edpuzzle's assignees, agents and subcontractors; provided that prior to any such disclosure, the assignee, agent or subcontractor receiving data has agreed in writing to comply with data protection obligations consistent with those applicable to Edpuzzle under applicable laws and regulations.

5.2. Edpuzzle shall assess the privacy and security policies and practices of third-party service providers to ensure such third-party service providers comply with best industry standards, including, but not limited to, ISO and NIST regulations.

5.3. Edpuzzle only sends personal identifiable information to third-party services that are required to support the service and fully attend Edpuzzle's user needs.

5.4. Edpuzzle's list of third-party service providers is maintained online and may be found in Edpuzzle's Privacy Policy.

5.5. In all cases, Edpuzzle shall impose the data protection terms on any third-party service provider it appoints that at a minimum meets the requirements provided for by the Agreement.

## 6. DATA STORAGE

6.1. The data is stored in externalized databases that are currently being provided by MongoDB Atlas (security compliance information), and simultaneously hosted on Amazon Web Services (security and compliance information) in North Virginia (United States).

6.2. User-generated content (which may or not contain personal information) may be temporarily stored in other countries in order for Edpuzzle to provide a better service. Concretely, uploaded videos, audios or images may have a copy temporarily stored in other regions to reduce the time of load. This would happen if, for example, a user accessed Edpuzzle from Europe and displayed a video created by an American teacher. In such a case, a temporary copy of such media would be hosted on the European server Amazon Web Services has in that region.

## 7. AGREEMENT EXPIRATION AND DISPOSITION OF DATA

7.1. The Service Agreement shall expire either (a) at District's request upon proactive deletion of user accounts; or (b) in the absence of any specific request or action, after eighteen (18) months of account inactivity. Deletion of student accounts must be requested by the District's authorized representative by sending a written request at [support@edpuzzle.com](mailto:support@edpuzzle.com) or [privacy@edpuzzle.com](mailto:privacy@edpuzzle.com).

7.2. The District will have the ability to download names, responses, results and grades obtained by students in their assignments ("Student Gradebooks") at any point prior to deletion. Except as otherwise provided in the laws, return or transfer of data, other than Student Gradebooks, to the District, shall not apply if proven to be incompatible with the Service, technically impossible or to involve a disproportionate effort for Edpuzzle. In such events, and upon written request by the District, Edpuzzle shall proceed to deletion of personally identifiable information in a manner consistent with the terms of this DSPPS, unless prohibited from deletion or required to be retained under state or federal law.

7.3. Without prejudice to the foregoing, Edpuzzle may keep copies and/or backups of data as part of its disaster recovery storage system for an additional term of thirteen (13) months after termination of services, provided such data is (a) inaccessible to the public; and (b) unable to be used in the normal course of business by Edpuzzle.

## 8. EDPUZZLE'S TERMS OF SERVICE AND PRIVACY POLICY

For all aspects not envisaged in this Data Security and Privacy Plan, Edpuzzle shall subject student data processing to its own Terms of Service and Privacy Policy, to the extent such documents do

not contravene the Agreement by any means, in which case the provisions foreseen in the Agreement shall prevail.

<b>TITLE</b>	Bolivar_Richburg-NY-DPA
<b>FILE NAME</b>	Copy of EdPuzzle ...t - BRCS.docx.pdf
<b>DOCUMENT ID</b>	c58ef9ef7ed809a97ecf5026230bb511daddcdcd
<b>AUDIT TRAIL DATE FORMAT</b>	MM / DD / YYYY
<b>STATUS</b>	● Completed

---

## Document history



SENT

**03 / 01 / 2021**

09:37:02 UTC

Sent for signature to Julia Trius (julia@edpuzzle.com) from jan@edpuzzle.com  
IP: 79.144.86.31



VIEWED

**03 / 09 / 2021**

12:10:53 UTC

Viewed by Julia Trius (julia@edpuzzle.com)  
IP: 88.1.174.120



SIGNED

**03 / 09 / 2021**

12:11:23 UTC

Signed by Julia Trius (julia@edpuzzle.com)  
IP: 88.1.174.120



COMPLETED

**03 / 09 / 2021**

12:11:23 UTC

The document has been completed.