

**AGREEMENT TO EXTEND
DATA PRIVACY AND SECURITY AGREEMENT**

WHEREAS, Agile Sports Technologies, Inc., having offices at 600 P Street, Suite 400, Lincoln, Nebraska 68508, hereinafter ("Contractor") and the Board of Cooperative Educational Services, Second Supervisory District of Erie, Chautauqua and Cattaraugus Counties, having its offices at 8685 Erie Road, Angola, New York 14006 ("E2CCB"), collectively "the Parties", agreed upon a Data Privacy and Security Agreement ("DPSA") that was signed on behalf of Contractor on September 14, 2021, and signed on behalf of E2CCB on September 23, 2021; and

WHEREAS, by written agreement dated May 10th, 2022 the Parties re-adopted and extended the above-referenced DPSA through June 30, 2024.


NOW, THEREFORE, it is agreed by and between Contractor and E2CCB that:

1. The DPSA (attached hereto as Attachment 1) is re-adopted and extended for the period July 1, 2024, through June 30, 2025 (the 2024-2025 school year).
2. All terms and conditions of the DPSA will remain in full force and effect, with the exception of the following:
 - a. The expiration date of the underlying agreement between the Parties, set forth in paragraph 7 of the DPSA, will be June 30, 2025.
 - b. Hudl will sign a revised copy of E2CCB's Parents Bill of Rights (attached hereto as Attachment 2), which will be unchanged from the version last signed by Hudl on September 14, 2021, except that the expiration date of the underlying agreement set forth in paragraph 3 will read "June 30, 2025."
3. The DPSA will be deemed to be a part of the renewed Agreement(s) for services between Contractor and E2CCB applicable during the 2024-2025 school year.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement to Extend the Data Privacy and Security Agreement on the dates set forth below.

Board of Cooperative Educational
Services, Second Supervisory District of
Erie, Chautauqua and Cattaraugus Counties

E2CCB


Bryna Moritz (Jul 2, 2024 11:43 EDT)

Signature

Bryna Moritz

Name

Deputy Superintendent

Title

Jul 2, 2024

Date

Agile Sports Technologies, Inc. dba
Hudl

CONTRACTOR


Signature

Tyler Kvasnicka

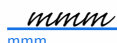
Name

Sales Manager

Title

6/26/2024

Date


mmmm




KD



ATTACHMENT 1

DATA PRIVACY AND SECURITY AGREEMENT

WHEREAS, Agile Sports Technologies, Inc., d/b/a Hudl, having its principal address at 600 P Street, Suite 400, Lincoln, Nebraska 68508 (hereinafter "Contractor") and the Board of Cooperative Educational Services, Second Supervisory District of Erie, Chautauqua and Cattaraugus Counties, having its offices at 8685 Erie Road, Angola, New York 14006 (hereinafter "E2CCB"), collectively "the Parties," are parties to an agreement addressing the terms on which E2CCB will purchase and distribute Hudl Software; and

WHEREAS, pursuant to that agreement, Contractor will receive student data and/or teacher or principal data in possession of E2CCB and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that contract with E2CCB for the use of Contractor's products and/or services; and

WHEREAS, in conformance with N.Y. Education Law § 2-d and 8 N.Y.C.R.R. § 121.1, *et seq.*, the Parties enter into this Data Privacy and Security Agreement (hereinafter the "Agreement") to address the confidentiality and security of student data and/or teacher or principal data received by Contractor.

NOW, THEREFORE, the Parties agree as follows:

1. For purposes of this Agreement, terms shall be defined as follows:
 - a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
 - b. "Commercial Purpose" or "Marketing Purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
 - c. "Disclose" or "Disclosure" means 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.
 - d. "Education Records" means 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.
 - e. "Eligible Student" means a student who is eighteen years or older.
 - f. "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.

- g. "Parent" means a parent, legal guardian, or person in parental relation to a student.
 - h. "Personally Identifiable Information," as applied to student data, 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 ("FERPA"), and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).
 - i. "Release" shall have the same meaning as Disclosure or Disclose.
 - j. "Student" means any person attending or seeking to enroll in an educational agency.
 - k. "Student data" means personally identifiable information from the student records of an educational agency. For purposes of this Agreement, "student data" includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies with whom E2CCB contracts.
 - l. "Teacher or principal data" means 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 N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this Agreement, "teacher or principal data" includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies with whom E2CCB contracts.
 - m. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.
2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:
- a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;
 - b. The terms and conditions of this Agreement, including but not limited to the E2CCB Parents Bill of Rights for Data Security and Privacy and the Supplemental Information to Parents Bill of Rights for Data Privacy and Security, attached hereto

as Exhibit A; and

- c. Applicable E2CCB policies, which can be accessed on the E2CCB website at: <https://go.boarddocs.com/ny/e2ccb/Board.nsf/Public>.

3. Contractor will use subcontractors in fulfilling its responsibilities to E2CCB, its employees or agents, and/or educational agencies which contract with E2CCB for the provision of Contractor's products and/or services. Any such subcontractors are required to execute legally binding agreements with Contractors acknowledging the subcontractor's obligation to comply with applicable state and federal laws, and data security and privacy standards that are at least as restrictive as those required of Contractor under this Agreement.

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state laws governing confidentiality of student data and/or teacher or principal data prior to receiving access to that data. More specifically, all of Contractor's employees are provided such training upon commencing employment and as necessary thereafter. As set forth in paragraph 3, above, any subcontractor with access to student data and/or teacher or principal data will be subject to training obligations at least as restrictive as those set forth herein.

5. The exclusive purpose for which Contractor is being provided student data and/or teacher or principal data, and for which such information will be used, is to provide the products and services for which E2CCB has contracted.

6. Student data and/or teacher or principal data received by Contractor, or by any subcontractor or assignee of Contractor, shall not be sold or used for any "commercial purpose" or "marketing purpose" as those terms are defined, above.

7. The agreement between Contractor and E2CCB for products and/or services expires on July 31, 2022. At the expiration of that agreement without a successor agreement in place, Contractor will either maintain any and all student data and/or teacher or principal data in its possession in accordance with the terms of this Agreement or assist E2CCB and/or the educational agency from which the data originated in transferring such data back to requesting educational agency. Additionally, upon request, Contractor shall securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the deletion or destruction of student data and/or teacher or principal data will be completed within 30 days of the request and will 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. To the extent that Contractor and/or its subcontractors or assignees may 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. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

8. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by E2CCB or the educational agency that generated the student data for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

9. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States or Canada, or in a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection. More specifically, Contractor has implemented the following administrative, operational, and technical safeguards:

- a. Prospective employees are subject to extensive screening, testing, interviews, and referral checking.
- b. All personnel, including third-parties, are subject to strict confidentiality agreements which form part of the contracts that are signed when they work for or with Contractor.
- c. Physical access to Contractor's offices requires individually assigned secure door-entry badges, with staffed reception desks and video surveillance cameras in use.
- d. For the purpose of data storage, Contractor utilizes Amazon Web Services, which has certification for compliance with ISO 27001, 27017, and 27018.
- e. Contractor utilizes malware protection systems in multiple locations, including within email message flows and on workstations.
- f. Contractor employs email content security solutions and other application aware systems to help protect against data leakage.
- g. Firewalls and virtual private networks help secure access to Contractor's systems,

with more sensitive data placed in logical silos.

- h. All Contractor's systems send logs to a single central analysis center for monitoring and review.

10. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided pursuant to its agreement with E2CCB, and any failure to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 N.Y.C.R.R. Part 121 shall also constitute a breach of its Agreement with E2CCB:

- a. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the Family Educational Rights and Privacy Act;
- b. Not use education records/and or student data for any purpose other than those explicitly authorized in this Agreement;
- c. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- e. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- f. Notify E2CCB of any breach of security resulting in an unauthorized release of student data by Contractor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but not more than seven (7) calendar days after discovery of the breach;
- g. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse E2CCB and/or any educational agencies which contract with E2CCB for the provision of Contractor's products or services for the cost of any notifications E2CCB and/or such other educational agencies is/are required to make by applicable law, rule, or regulation; and

- h. Contractor will cooperate with E2CCB and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
- i. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Contractor by state and federal law, and by this Agreement, shall apply to the subcontractor.

11. Contractor has measures in place to identify breaches and/or unauthorized disclosures of student data and/or teacher or principal data, which will include managing risks on a real-time basis with regular formal reviews, monitoring its systems for vulnerabilities in underlying products, and patching all critical vulnerabilities. In the event of a data security and privacy incident (including but not limited to a breach, unauthorized release, and/or unauthorized disclosure) implicating the personally identifiable information of students, teachers, and/or principals of E2CCB or educational agencies which contract with E2CCB for the provision of Contractor's products or services, Contractor will respond in accordance with its internal security incident management processes. Such processes will include, at minimum, investigating the nature and extent of the incident, taking remedial measures to prevent further vulnerabilities, and notifying E2CCB in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and paragraph 10(f), above.

12. Contractor, its employees and representatives shall at all times comply with all federal, state, and local laws, rules, and regulations applicable to the provision of Contractor's products and services under this Agreement.

13. This Agreement, together with the (i) Hudl Organization Terms of Service found at www.hudl.com/eula (the "Org Terms"); (ii) signed Parents Bill of Rights for Data Privacy and Security; and (iii) Supplemental Information to Parents Bill of Rights for Data Privacy and Security, constitute the entire understanding of the Parties with respect to the subject matter thereof. The terms of this Agreement, together with the signed Parents Bill of Rights for Data Privacy and Security and the Supplemental Information to Parents Bill of Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor's Org Terms.

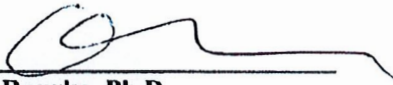
14. If any provision of this Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision to this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

15. This Agreement shall be binding on any successors of the parties. Neither party shall have the right to assign its interests in the Agreement to any other party, unless the prior written consent of the other party is obtained; provided, however, that Contractor may assign this Agreement to an affiliate or a successor-in-interest by consolidation, merger, or operation of law or to a purchaser of all or substantially all of Contractor's assets. No assignment shall relieve Contractor of any of its obligations hereunder.

16. This Agreement shall be governed by the laws of the State of New York. Any action or proceeding arising out of this contract shall brought in the appropriate courts of New York State.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Memorandum on the date indicated.

**FOR THE ERIE 2-CHAUTAUQUA-
CATTARAUGUS BOCES:**




David O'Rourke, Ph.D.
District Superintendent

9.23.2021

Date

**FOR THE CONTRACTOR: AGILE
SPORTS TECHNOLOGIES, INC.**



McKenzie Swanson
Manager, Competitive Sales

09/14/2021

Date

ATTACHMENT 2: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

E2CCB is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, E2CCB wishes to inform the community of the following:

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.
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 for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or 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 have complaints about possible breaches of student data addressed. Complaints may be submitted to NYSED at www.nysed.gov/data-privacy-security; 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.

Supplemental Information to Parents Bill of Rights for Data Privacy and Security:

1. The exclusive purpose for which Agile Sports Technologies, Inc., d/b/a Hudl (hereinafter "Contractor") is being provided student data and/or teacher or principal data, and for which such information will be used, is to provide the products and services for which E2CCB has contracted. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from E2CCB or its employees, officers, agents, and/or students will not be sold or used for commercial purpose or marketing purpose.
2. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, all of Contractor's employees are provided such training upon commencing employment and as necessary thereafter. Any subcontractors engaged by Contractor, and which have access to student data and/or teacher or principal data, are required to execute legally binding agreements with Contractors acknowledging the subcontractor's obligation to comply with data security and privacy standards at least as restrictive as those required of Contractor under

the Data Privacy and Security Agreement between E2CCB and Hudl, as well as applicable state and federal law.


3. The agreement between Contractor and E2CCB for products and/or services expires on June 30, 2025. At the expiration of that agreement without a successor agreement in place, Contractor will either maintain any and all student data and/or teacher or principal data in its possession in accordance with the terms of this Agreement or assist E2CCB and/or the educational agency from which the data originated in transferring such data back to requesting educational agency. Additionally, upon request, Contractor will securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the deletion or destruction of student data and/or teacher or principal data will be completed within 30 days of the request and will 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. To the extent that Contractor and/or its subcontractors or assignees may 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. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.
4. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the E2CCB for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the BOCES Annual Professional Performance Review Plan.
5. Student data and/or teacher or principal data transferred to Contractor by E2CCB or E2CCB officers, employees, agents, or students will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection. More specifically, Contractor has implemented the following administrative, operational,

and technical safeguards:

- a. Prospective employees are subject to extensive screening, testing, interviews, and referral checking.
 - b. All personnel, including third parties, are subject to strict confidentiality agreements which form part of the contracts that are signed when they work for or with Contractor.
 - c. Physical access to Contractor's offices requires individually assigned secure door-entry badges, with staffed reception desks and video surveillance cameras in use.
 - d. For the purpose of data storage, Contractor utilizes Amazon Web Services, which has certification for compliance with ISO 27001, 27017, and 27018.
 - e. Contractor utilizes malware protection systems in multiple locations, including within email message flows and on workstations.
 - f. Contractor employs email content security solutions and other application aware systems to help protect against data leakage.
 - g. Firewalls and virtual private networks help secure access to Contractor's systems, with more sensitive data placed in logical silos.
 - h. All Contractor's systems send logs to a single central analysis center for monitoring and review.
6. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest.

Acknowledged and agreed to by:

Signature:



Name:

Tyler Kvasnicka

Title:

Sales Manager

Date:

6/26/2024












2024-2025 Hudl DPA

Final Audit Report

2024-07-02

Created:	2024-06-27
By:	Tamala Sweet (tsweet@e2ccb.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAsv-MLGJUjkQ-8OdPNAmCK3DJxQku6jTk

"2024-2025 Hudl DPA" History

-  Document created by Tamala Sweet (tsweet@e2ccb.org)
2024-06-27 - 4:21:31 PM GMT- IP address: 74.84.250.191
-  Document emailed to Tamala Sweet (tsweet@e2ccb.org) for approval
2024-06-27 - 4:24:00 PM GMT
-  Document approved by Tamala Sweet (tsweet@e2ccb.org)
Approval Date: 2024-06-27 - 4:24:23 PM GMT - Time Source: server- IP address: 74.84.250.191
-  Document emailed to Matthew Moore (mmoore@e2ccb.org) for approval
2024-06-27 - 4:24:26 PM GMT
-  Email viewed by Matthew Moore (mmoore@e2ccb.org)
2024-06-27 - 4:34:59 PM GMT- IP address: 168.169.223.96
-  Document approved by Matthew Moore (mmoore@e2ccb.org)
Approval Date: 2024-06-27 - 4:35:16 PM GMT - Time Source: server- IP address: 168.169.223.96
-  Document emailed to Robin Brown (rbrown@e2ccb.org) for approval
2024-06-27 - 4:35:19 PM GMT
-  Email viewed by Robin Brown (rbrown@e2ccb.org)
2024-06-27 - 5:47:55 PM GMT- IP address: 66.249.83.89
-  Document approved by Robin Brown (rbrown@e2ccb.org)
Approval Date: 2024-06-28 - 12:08:36 PM GMT - Time Source: server- IP address: 168.169.223.96
-  Document emailed to Deneen Lalock (DLalock@e2ccb.org) for approval
2024-06-28 - 12:08:39 PM GMT
-  Email viewed by Deneen Lalock (DLalock@e2ccb.org)
2024-06-28 - 2:31:35 PM GMT- IP address: 74.125.210.5



Document approved by Deneen Lalock (DLalock@e2ccb.org)

Approval Date: 2024-06-28 - 2:32:27 PM GMT - Time Source: server- IP address: 168.169.223.96



Document emailed to Karen Drummond (kdrummond@e2ccb.org) for approval

2024-06-28 - 2:32:30 PM GMT



Email viewed by Karen Drummond (kdrummond@e2ccb.org)

2024-06-28 - 3:16:47 PM GMT- IP address: 66.249.83.76



Document approved by Karen Drummond (kdrummond@e2ccb.org)

Approval Date: 2024-06-28 - 3:17:01 PM GMT - Time Source: server- IP address: 168.169.223.96



Document emailed to Terri Iskra (teiskra@e2ccb.org) for approval

2024-06-28 - 3:17:04 PM GMT



Email viewed by Terri Iskra (teiskra@e2ccb.org)

2024-07-01 - 1:18:10 PM GMT- IP address: 66.249.83.64



Document approved by Terri Iskra (teiskra@e2ccb.org)

Approval Date: 2024-07-01 - 1:18:17 PM GMT - Time Source: server- IP address: 168.169.221.96



Document emailed to John Griesmer (JGriesmer@e2ccb.org) for approval

2024-07-01 - 1:18:19 PM GMT



Email viewed by John Griesmer (JGriesmer@e2ccb.org)

2024-07-01 - 1:54:14 PM GMT- IP address: 74.125.210.6



Document approved by John Griesmer (JGriesmer@e2ccb.org)

Approval Date: 2024-07-01 - 2:17:56 PM GMT - Time Source: server- IP address: 174.211.228.57



Document emailed to Lindsay Anderson (LAnderson@e2ccb.org) for approval

2024-07-01 - 2:17:59 PM GMT



Email viewed by Lindsay Anderson (LAnderson@e2ccb.org)

2024-07-01 - 2:24:31 PM GMT- IP address: 66.249.83.89



Document approved by Lindsay Anderson (LAnderson@e2ccb.org)

Approval Date: 2024-07-01 - 2:24:37 PM GMT - Time Source: server- IP address: 168.169.221.96



Document emailed to Bryna Moritz (bmoritz@e2ccb.org) for signature

2024-07-01 - 2:24:40 PM GMT



Email viewed by Bryna Moritz (bmoritz@e2ccb.org)

2024-07-02 - 3:43:20 PM GMT- IP address: 66.249.83.89



Document e-signed by Bryna Moritz (bmoritz@e2ccb.org)

Signature Date: 2024-07-02 - 3:43:37 PM GMT - Time Source: server- IP address: 174.208.32.64



Adobe Acrobat Sign

✔ Agreement completed.

2024-07-02 - 3:43:37 PM GMT