



## II. Order Form

Client Name: Boone County Schools, KY	
Address: 8330 US HWY 42, Florence	Email: kathy.reutman@boone.kyschools.us
Kentucky 41042	Phone: 859-334-4466

Description	Price	Qty	Subtotal
<b>Mobile App + Web Development (one-time)</b> One-time app development for iOS and Android apps for the District + 27 campuses *Billed one-time	\$14,500	1	\$14,500
<b>App Development Discount (one-time)</b> Discounting app development for agreement signed by (3/31/2025)	-\$8,500	1	-\$8,500
<b>Thrillshare - Suite (annual)</b> Thrillshare Publishing Platform (desktop and mobile) for ~20,000 students *Billed and payable in full annually  Includes Thrillshare Media and Thrillshare Rooms  *For Clients that elect automatic renewal, pricing subject to 5% annual increases after last year of initial purchased term(see Terms for more info)	\$99,000	1	\$99,000
<b>Alerts</b> Unlimited text, voice, and email alerts Included in Thrillshare cost  *Subject to Carrier restrictions (see Terms for more info), including, but not limited to, character limits per SMS message [currently 320 characters per SMS message]	\$0	1	\$0
<b>Engage (annual)</b> Newsletters, Forms, and ongoing Training and support *Billed and payable in full annually *For Clients that elect automatic renewal, pricing subject to 5% annual increases after last year of initial purchased term(see Terms for more info)	\$0	1	\$0
<b>Support, service, and training</b> Included in Thrillshare cost Includes unlimited training for up to 10 staff users	\$0	1	\$0



### III. Payment Schedule

Payment Schedule: Payable subject to the terms of Agreement	Amount
Total of the above, collectively, the "Services"	\$105,000.00
Billed after signature	\$6,000 (one-time development cost)
7/01/2025 ("Client Start Date")	\$99,000 (annual)
One year from Client Start Date	\$99,000 (annual, if renewed) <small>*Subject to 5% increase for renewal</small>

This Order Form and Master Services Agreement (collectively, the "Agreement") between Apptegy, Inc. ("Apptegy"), and the client listed above ("Client") is effective as of the date of Client's signature below. This Agreement includes and incorporates the above Order Form, as well as the attached Master Services Agreement ("MSA"). By signing below, Client acknowledges receipt of this Agreement, including the Order Form and the MSA, and hereby accepts and agrees to be bound by this Agreement.

Client

By:  SIGNATURE  
Kathleen Reutman

Name: Kathleen Reutman

Title: Executive Director

Date:

Apptegy, Inc.

By:   
2025-01-24 14:47:59 (CST)

Name: Dutch King

Title: Sales Representative



## Master Services Agreement

The following terms and conditions are a binding part of the Order Form and Master Services Agreement of Apptegy, Inc. (together with its affiliates, agents, and assigns, "**Apptegy**") between Apptegy and the Client that is set out in the Order Form. References to the "**Agreement**" below collectively include the Order Form (including and incorporating the terms and conditions set out in the "**Estimated Transition Timeline**" and the "**Payment Schedule**" that is provided with this Agreement) and the following terms and conditions. This Agreement provides the terms and conditions for Client to purchase and use Apptegy's Services (as defined below). Capitalized terms used but not otherwise defined in the following terms and conditions will have the meanings given to them in the Order Form.

**1. Integration with Other Documents.** This Agreement is the entire agreement between Apptegy and Client with respect to the Services, except as expressly set out below. No separate written or online agreements or terms and conditions will be incorporated in this Agreement or otherwise bind the parties unless expressly set out in this Agreement or in a Client Addendum (as defined below). The Client Addendum will control and govern with respect to all matters expressly set out in the Client Addendum, and this Agreement will control and govern in all circumstances. To be enforceable on the parties, any amendment, modification, or additions to the terms and conditions of this Agreement must be set out in a separate written addendum to this Agreement confirming such amendments, modifications, and/or additions in writing (a "**Client Addendum**").

**2. Services; License.** During the License Term, Apptegy will provide, and Client and the individuals allowed to access the Services by or on behalf of Client ("**User(s)**") may access and use, the products and services set out in the Order Form (collectively, "**Services**"). Client hereby grants Apptegy a limited, nonexclusive, revocable, worldwide, fully-paid, royalty-free license to use, copy, and modify Client's information, material, data, photographs, videos, intellectual property (including without limitation all copyrights, trademarks, service marks, and similar rights), and other content (collectively, "**Client Content**") for providing and improving the Services. Client's right to access and use the Services, and Apptegy's license to Client Content, will automatically terminate upon termination or expiration of this Agreement.

**3. Fees.** Client will pay to Apptegy all fees set out in the Order Form. Apptegy will submit invoice(s) to Client for all fees due upon execution of the Agreement and/or on the Client Start Date(s) (as defined below) as set out in the Order Form. Apptegy will invoice all subsequent-year fees on or about the anniversary of the applicable Client Start Date(s). Client agrees to pay all invoices in full within 30 days of the date of the invoice. Client agrees that (i) development and implementation fees are due as set out in the Order Form, (ii) fees for use of the Services are payable in annual portions for each year of the License Term as set out in the Order Form, (iii) fees for use of the Services are subject to Five Percent (5%) annual increases, starting the first renewal year after the last year of the term initially purchased by Client and continuing each year thereafter, as set out in the Order Form, and (iv) discounts for purchases of bundled Services will automatically expire if Client cancels any of the bundled Services and Client will thereafter be invoiced for the full price of the continuing Services. Client acknowledges that fees for Services do not include taxes, duties, and other government charges, including sales, use, consumption, VAT, GST, and other withholding, as applicable, and Client is solely responsible for any such obligations.

**4. License Term.** The term of Client's license to use the Services (the "**License Term**") will start on the date(s) set out on the Order Form (the "**Client Start Date(s)**"). Clients that purchase multiple Apptegy products may have different license start dates for different products. If no license start date is set out on the Order Form, the Thrillshare Media Client Start Date will be the date that is 60 days after Apptegy receives an executed agreement from Client and the Thrillshare Rooms Client Start Date will be the date that is 90 days after Apptegy receives an executed agreement from Client. The License Term will terminate on the anniversary of the applicable Client Start Date(s) that is after the number of license years initially purchased by Client, as set out in the Order Form, plus any renewal periods. This Agreement will renew for successive, additional periods of one (1) year from the anniversary of the Client Start Date(s), unless Client provides Apptegy with written notice of non-renewal before the end of the then-current License Term. Subject only to applicable procurement and appropriations law, Client agrees that it may not terminate this Agreement before the expiration of any then-current License Term without cause, unless Client pays Apptegy all fees in full for all license years of the then-current License Term, as set out in the Order Form, plus payment of any previously discounted amounts for the Services during the Term. All fees paid to Apptegy are non-refundable, subject only to applicable procurement and appropriations law.

**5. Performance Terms.** In addition to this Agreement, the rights and obligations of the Client and Apptegy with respect to the providing, accessing, and using the Services will also be subject to and governed by the Apptegy Terms of Use ("**Terms of Use**") and Privacy Policy ("**Privacy Policy**"), available at the following links: <https://www.apptegy.com/terms-and-conditions/> and <https://www.apptegy.com/privacy-policy/>. The Terms of Use and Privacy Policy, as each may be amended, are incorporated into this Agreement in their entirety, as applicable to Client. Without limiting the generality of the foregoing, the Terms of Use and Privacy Policy set out and govern the terms and conditions for Services availability, User eligibility and acceptable use, data privacy and security, regulatory notices and information, warranties, disclaimers, and liability limitations, and other related terms. The applicability of the Terms of Use and Privacy Policy is limited to the order of priority set out below.

**6. Carrier Restrictions.** Apptegy provides unlimited text, voice, and email messaging to Client subject to restrictions placed on Apptegy by mobile and wireless carriers and network operators (collectively, "**Carriers**"). For example, Carriers have (i) placed limits on the number of characters that may be included in messages sent via the Services and (ii) placed restrictions on the type of messaging content that may be sent through the Services. Carrier restrictions are not within the control of Apptegy and are subject to change without notice. When a Carrier places new or modified restrictions on Apptegy, certain features and functions of the Services may change as a result without notice to you. Client agrees that Apptegy will not be responsible or liable for any change in Services that arise from or in connection with Carrier restrictions.

**7. TCPA/CTIA Compliance.** Client is exclusively responsible for complying with applicable laws and regulations governing communications sent via the Services by Client and Users under Client's account, including, but not limited to, the Telephone Consumer Protection Act of 1991, as it may be amended ("**TCPA**"), and the requirements and policies of CTIA – The Wireless Association ("**CTIA**"). Client is encouraged to establish and implement methods and procedures to ensure compliance with applicable laws and regulations, including the TCPA and the CTIA, and to inform and train each of its employees, contractors, and representatives who use the Services on the methods and procedures. Apptegy may provide Client with materials and information about such laws and regulations, including the TCPA and the CTIA;

Client acknowledges that all such materials and information is provided for general education purposes only. No such act by or information from Apptegy (whether individually or taken as a whole) will create or be deemed to create responsibility or liability on the part of Apptegy with respect to Client's compliance with the laws and regulations governing the communications sent via the Services by Client and Users under Client's account, including the TCPA and/or the CTIA.

**8. COPPA Notice and Compliance.** Apptegy prohibits use of the Services by children under the age of thirteen (13), unless and only to the extent the child is a User invited or added to the Services by Client. When children are invited or added to the Services as Users under Client's account, Apptegy provides the Services with respect to the children solely in the educational context authorized by Client under this Agreement and solely for the benefit of Client and its Users. Client consents, as agent for and on behalf of such children (and their parents and guardians), to Apptegy's collection, use, disclosure, and storage of personal information about or from the children in accordance with this Agreement. Client acknowledges that Apptegy is relying on Client's consent in the previous sentence for the purposes of complying with the Children's Online Privacy Protection Act, as it may be amended ("**COPPA**"), and that Apptegy is authorized to presume that Client has obtained and will maintain all required parent and guardian consent for Apptegy's collection, use, disclosure, and storage of information for any children under the age of thirteen (13) that are invited or added to the Services under Client's account.

Please note that Client is responsible for complying with COPPA with respect to Users under Client's account if Client invites or adds children under the age of thirteen (13) to the Services. Client is encouraged to establish and implement methods and procedures to ensure compliance with COPPA, and to inform and train each of its employees, contractors, representatives, and Users who use the Services on the methods and procedures. Apptegy may provide Client with materials and information about complying with COPPA; Client acknowledges that all such materials and information is provided for general education purposes only. No such act by or information from Apptegy (whether individually or taken as a whole) will create or be deemed to create responsibility or liability on the part of Apptegy with respect to Client's compliance with COPPA.

The Terms of Use and Privacy Policy, accessible as set out above, confirm that Apptegy may collect information about children as a necessary part of providing the Services to Client (for example, as applicable: contact information for communications sent via the Services;

posts made on messaging tools in the Services; information included in assignments and other class content submitted via the Services) and provide notice regarding Apptegy's collection, use, disclosure, and storage of personal information from children. Please note that some or all of this information may not be private as to the individual child, parent, or guardian. For example, for Users of Rooms, information shared by a User via the messaging features of Rooms will be visible to Client, as the party providing access to the Services to its Users. In some circumstances, information provided by or about a child may be available or visible to other individual Users. For example, for Users of Rooms, information about a child that is posted in the group messaging tool in a Child's Room may be visible to other individual Users that are also authorized users for the same Room. Apptegy will collect, use, and disclose such information in accordance with COPPA and the Privacy Policy.

**9. Accessibility Compliance.** Client is exclusively responsible for complying with all applicable laws and regulations governing accessibility of the parts of the Services under the control of Client (for example: Client's website and/or mobile applications), including, but not limited to, the Americans with Disabilities Act, as it may be amended ("**ADA**"), and the requirements and policies of Web Content Accessibility Guidelines ("**WCAG**"). Client is encouraged to establish and implement methods and procedures to ensure compliance with applicable laws and regulations, including the ADA and the WCAG, and to inform and train each of its employees, contractors, and representatives who use the Services on the methods and procedures. The Services include tools to assist Client with accessibility compliance, and Apptegy may provide Client with materials and information about such laws and regulations, including the ADA and the WCAG; Client acknowledges that all such tools, materials, and information are provided to assist Client with its compliance obligations and for general education purposes only. No such functionality, act by, or information from Apptegy (whether individually or taken as a whole) will create or be deemed to create responsibility or liability on the part of Apptegy with respect to Client's compliance with the laws and regulations governing accessibility of the parts of the Services under the control of Client (for example: Client's website and/or mobile applications), including the ADA and/or the WCAG.

**10. Third Party Functions.** Apptegy relies on third-party providers and partners for parts of the Services (for example: posting a message or communication on Facebook or Twitter account; hosting Client websites). APPTEGY IS NOT RESPONSIBLE FOR ANY CONSEQUENCE, LOSS, OR DAMAGE (DIRECT OR INDIRECT) ARISING FROM OR RELATING TO THE PARTS OF THE SERVICES MANAGED OR MADE AVAILABLE BY OR VIA THIRD-PARTY PROVIDERS AND PARTNERS. Please see the Terms of Use and Privacy Policy for more information.

**11. Disclaimers; Limited Liability.** Apptegy provides the Services subject to certain disclaimers and limitations of liability. Please see the Terms of Use and Privacy Policy for more information.

**12. Intellectual Property.** Nothing in this Agreement or the performance of this Agreement will convey, license, or otherwise transfer any right, title, or interest in any intellectual property or other proprietary rights held by either party, except as expressly set out in the Agreement. Apptegy retains all right, title, and interest in all intellectual property rights, including patent, trademark, trade secret, and copyright (whether registered or unregistered), in and to the Services and the underlying software and technologies, all related technical documentation, and all derivative works, improvements, and modifications to any of the foregoing. Client agrees the foregoing is necessary to Apptegy providing the Services.

**13. Compliance with Laws.** The parties agree to comply with all laws applicable to the use of the Services and performance of this Agreement.

**14. Miscellaneous.** The Order Form and Master Services Agreement, together with (i) the Terms of Use and Privacy Policy, and (ii) the Client Addendum, if applicable, is the entire agreement between the parties with respect to the subject matter, and supersedes all prior agreements and understandings, whether written or oral. If any conflict or ambiguity exists with respect to any term or condition of any of the foregoing, the following priority will govern and control: (1) if applicable, the Client Addendum for all matters expressly addressed in the Client Addendum; then (2) this Order Form and Master Services Agreement for all other matters; then (3) the Terms of Use and Privacy Policy. Apptegy is not subject to any obligations that are not expressly identified in this Agreement, a Client Addendum, or the Terms of Use and Privacy Policy.

This Agreement is governed by the laws of the state in which Client is located, without regard to conflict of law principles. The parties irrevocably submit to the exclusive jurisdiction and venue of the federal courts having jurisdiction where Client is located for any dispute that relates to the Services or this Agreement. Except as set out in this Agreement, this Agreement may not be amended or modified without the prior written consent of both parties.



Neither party may assign this Agreement without the prior written consent of the other party, except in connection with a merger, acquisition, or sale of all or substantially all of a party's assets or voting securities. If any provision(s) of this Agreement is held invalid or unenforceable, such invalidity or unenforceability will not invalidate or render the Agreement unenforceable, but rather the Agreement will be construed as if not containing the unenforceable provision(s), and the rights and obligations of the parties will be construed and enforced to honor the parties' original intent to the maximum extent permitted under applicable law. This Agreement will inure to the benefit of the successors and assigns of the parties. The Agreement may be executed in multiple counterparts and executed by original, facsimile, or electronic signature (including PDF, Proposify, HelloSign, and similar methods), each of which when delivered will be deemed an original, and all of which together will constitute one agreement.



## **Data Privacy and Security Agreement**

This Data Privacy and Security Agreement (“Agreement”) is agreed and entered into by and between the Boone County School District (“District”) and Apptegy, Inc. (“Vendor”) on this the 12<sup>th</sup> day of February, 2025.

**WHEREAS**, Boone County School District (“District”) is a public school district organized and existing under and pursuant to the constitution and laws of the State of Kentucky and with a primary business address at 8330 US Highway 42, Florence, KY 41042; and

**WHEREAS**, Vendor has been contracted to perform certain educational services as described fully in Exhibit A (“Provided Services”) with a primary place of business at 2201 Brookwood Dr., Ste. 115, Little Rock, AR 72202 and

**WHEREAS**, the Vendor and the District recognize the need to protect personally identifiable student information, and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232(g), 34 C.F.R. Part 99; the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 6501-6506, 16 C.F.R. Part 312; the Protection of Pupil Rights Amendment (“PPRA”), 20 U.S.C. § 1232h; 34 C.F.R. Part 98; and applicable state privacy laws and regulations; and

**WHEREAS**, the Vendor and District desire to enter into this Agreement for the purpose of establishing their respective obligations and duties in order to comply with applicable regulations; and

**WHEREAS**, the Parties acknowledge that this Agreement shall amend, modify, and supplement any agreement or terms previously entered into; and

**NOW THEREFORE**, in consideration of the of the terms, covenants, conditions and promises set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

### **Section 1. DEFINITIONS**

1.1 “Confidential Student Information” shall mean any information or material, in any medium or format, that concerns a student and is created or provided by the student, or by an agent or employee of the District. Confidential Student Information includes both PII and directory information.

1.2 “De-identified Data” shall mean data that has a re-identification code and has enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that

the information can be used to identify an individual. The re-identification code may allow the recipient to match information received from the same source.

1.3 “District Data” shall mean any information or data owned by the District and provided to Vendor pursuant to the Parties’ Agreement, including but not limited to Confidential Student Data and PII. District Data shall not include De-Identified Data.

1.4 “Education Records” shall be defined consistent with the definition set forth in 20 U.S.C. § 1232g(a)(4)(A); 34 C.F.R. § 99.3, and shall mean records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.

1.5 “Personally Identifiable Information” (“PII”) shall be defined consistent with the definition set forth in 20 U.S.C. § 1232g(a); 34 C.F.R. § 99.3, and shall mean identifiable information that is maintained in Education Records and includes direct identifiers, such as a student’s name or identification number, indirect identifiers, such as a student’s date of birth, or other information which can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information.

1.6 “Personal Information” shall be defined in accordance with KRS 61.931(6) as an individual’s first name or first initial and last name; personal mark, or unique biometric or genetic print or image in combination with one (1) or more of the following data elements: (1) an account, credit card number, or debit card number that in combination with any required security code, access code or password, would permit access to an account; (2) a Social Security number; (3) a taxpayer identification number that incorporates a Social Security number; (4) a driver’s license number, state identification card number, or individual identification number issued by an agency; (5) A passport number or other identification number issued by the United States Government; or (6) Individually Identifiable Information as defined in 45 C.F.R. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

## **Section 2. PURPOSE AND SCOPE**

2.1 The purpose of this Agreement is to allow the District to provide the Vendor with student and teacher PII data and the subsequent processing of the data.

2.2 This Agreement is meant to ensure the Vendor and the District recognize the need to protect PII, and other regulated data exchanged between them as required by applicable laws and regulations, such as FERPA, 20 U.S.C. § 1232(g), 34 C.F.R. Part 99; the COPPA, 15 U.S.C. § 6501-6506, 16 C.F.R. Part 312; PPRa, 20 U.S.C. § 1232h; 34 C.F.R. Part 98; and applicable state privacy laws and regulations; and

2.3 This Agreement shall be effective as of the date upon which it is signed by both parties (“Effective Date”), and shall automatically renew from year to year, unless otherwise modified in writing and signed by each party. This Agreement shall remain in full force and effect at all times during which Vendor supplies Provided Services to the District.

2.4 The laws of the Commonwealth of Kentucky shall govern all questions as to the execution, validity, interpretation, construction, and performance of this Agreement and any of its terms. Any suit, action, or other proceeding regarding the execution, validity, interpretation, construction, or performance of this agreement shall be filed in the Boone Circuit Court of the Commonwealth of Kentucky. In the event of litigation in a U.S. District Court, the venue shall lie exclusively in the Eastern District of Kentucky.

### **Section 3. DISTRICT DUTIES**

The District shall provide data as required for Vendor to conduct its Provided Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations. To the extent appropriate or applicable, District shall assist Vendor in securing any parent permissions regarding the use of Confidential Student Information or PII.

### **Section 4. VENDOR DUTIES**

4.1 Vendor acknowledges that the District has outsourced certain services to Vendor, as defined above as Provided Services, in furtherance of a legitimate educational interest that would otherwise be performed by the school district, enabling Vendor to act in the capacity of a school official for the limited purpose of performing services pursuant to the parties’ underlying agreement, as contemplated by FERPA. These Provided Services necessitate the collection and storage of certain District Data and Confidential Student Information. Vendor shall act as a contractor to the District in performing the Provided Services, either directly under the terms of any service or licensing agreement related to the Provided Services, or indirectly through the Vendor’s interfaces with another District contractor, and Vendor therefore acknowledges that it is subject to the requirements in FERPA that any PII obtained from Education Records may be used only for the purposes for which the disclosure was made and solely for the purpose of performing the Provided Services.

4.2 Vendor shall implement commercially reasonable methods to ensure that District Data is accessed, used, and manipulated exclusively by authorized individuals with a legitimate educational interest—such as the student, the student’s guardian, and the District—or by personnel essential for the successful performance and execution of the Provided Services. No unauthorized third parties shall have access to Confidential Student Information or Education Records in Vendor’s control unless written authorization to distribute such information is provided by the student’s parent/guardian. Such unauthorized third parties will not include Vendor’s subprocessors, necessary for Vendor’s

Provided Services, as described in Vendor's Privacy Policy ("Privacy Policy") (<https://www.apptegy.com/privacy-policy/>) and Terms of Use (<https://www.apptegy.com/terms-of-use/>) ("Terms of Use"). Such Privacy Policy and Terms of Use are incorporated herein in their entirety, and to the extent there are any inconsistencies, this Agreement shall prevail. Vendor agrees that it shall require any subprocessors with access to Confidential Student Information to enter into written agreements containing obligations of confidentiality that are no less stringent than those set forth in this Agreement. In the event that Vendor engages a third party subprocessor to provide elements of the Provided Service and shares District Data with said third party, Vendor shall indemnify, defend, and hold harmless the District, its officers, directors, employees, and agents from and against any and all claims, demands, actions, suits, proceedings, liabilities, losses, damages, judgments, settlements, costs, and expenses (including reasonable attorneys' fees and costs of investigation) stemming from the third party's gross negligence or intentional misconduct resulting in an actual or reasonably suspected security breach of District Data. Notwithstanding the foregoing, Vendor shall only be liable to District for the gross negligence or intentional misconduct of a third party subprocessor to the extent such liability is covered by Vendor's cyber-insurance liability policy. Such liability is limited to the amount determined by the applicable insurer as covered and available under the policy at the time of the claim. For avoidance of doubt, Vendor shall not be liable for claims or amounts not covered, as determined by and at the sole discretion of the applicable insurer, or amounts exceeding the minimum policy limit required by this Agreement.

4.3 Vendor shall likewise implement commercially reasonable measures to safeguard data at rest, and advise all individuals accessing the data on proper procedures for securely maintaining data. Vendor shall adhere to valid encryption processes for data at rest that are consistent with NIST Special Publication 800-111 and comply with relevant data protection regulations to ensure the confidentiality and integrity of data at rest. If requested by the District, the Vendor shall provide a list of locations where student data is/may be stored, and whenever possible, including where required by applicable law, data shall be stored within the United States.

4.4 The Vendor shall ensure the secure transmission of any data exchanged during the course of this agreement. All data transmissions, whether internal or external, shall be encrypted using encryption processes for data in motion which comply, as appropriate, with National Institute of Standards and Technology ("NIST") Special Publications 800-52; NIST Special Publications 800-77; NIST Special Publications 800-113, or others which are Federal Information Processing Standards ("FIPS") 140-2 validated, to protect the confidentiality and integrity of the transmitted data. In the event of any security incidents or breaches

affecting data while in transit, the Vendor agrees to promptly notify the District and take necessary remedial actions to mitigate the impact, as set forth in Section 6 of this Agreement.

4.5 In the event of any security incidents or potential or actual breaches affecting the security of District Data, the Vendor agrees to promptly notify the District and take necessary remedial actions to mitigate the impact as set forth in Section 6 of this Agreement.

4.6 Upon termination, cancellation, expiration, or other conclusion of the Parties' contractual relationship, or upon receipt of written request from District, Vendor shall delete all Confidential Student Data in its possession. Vendor shall complete such return or destruction within sixty (60) calendar days of the receipt of the written request and shall certify compliance with this Section, in writing, to the District within ten (10) calendar days of such destruction.

4.7 Vendor is prohibited from using, disclosing, or selling Confidential Student Information or District Data to any unauthorized individual or entity, or for any purpose which is not required in the performance of Vendor's Provided Services. This does not prohibit Vendor from using Confidential Student Information or District Data: (a) for adaptive learning or customized student learning (including generating personalized learning recommendations); (b) to make product recommendations to teachers or District employees who have voluntarily subscribed to Vendor's Provided Services; (c) to notify account holders about new education product updates, features, or services; or (d) from otherwise using Confidential Student Information or District Data for any purpose explicitly permitted by the Parties' Agreement. However, Vendor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purpose and shall not sell, disclose, or otherwise process student data for any commercial purpose as defined by KRS 365.734.

4.8 Vendor acknowledges and agrees that it may not disseminate any Confidential Student Information or District Data – whether explicitly protected under FERPA, directory information (i.e., name, grade, etc.), or student likeness – without written authorization from the student or, if the student is a minor, the student's parent/guardian, except to necessary employees or subprocessors, solely for Vendor to provide the Provided Services. Vendor likewise acknowledges and agrees that it may not disseminate the District's name, logo, or likeness for any reason, including marketing, internal training, or similar purposes, to any third party without written authorization from the District.

4.9 Vendor shall maintain, during the term of the Agreement, a cyber-insurance liability policy, in the amount of \$3 million. Upon request, the Vendor shall furnish the certificate of insurance evidencing this coverage.

4.10 To the extent permitted by law and not inconsistent with the underlying agreement between the parties, Vendor assumes all liability for damages which may arise directly from its grossly negligent or willful misuse, storage, or disposal of the District Data. The District shall not be liable to the Vendor for any loss, claim or demand made by the Vendor, or made against the Vendor by any other party, due to or arising from the use of data by the Vendor, except to the extent permitted by law when caused by gross negligence or willful misconduct of the District.

4.11 To the extent not inconsistent with the terms set forth in the underlying agreement between the parties, Vendor shall defend, indemnify, and hold harmless the District, its agencies, officers, and employees from any and all claims of any nature, including all costs, expenses, and attorney's fees, which may in any manner directly result from or arise out of this Vendor's gross negligence or willful misconduct in performance of this Agreement, except for claims resulting from or arising out of the District's sole negligence. The legal defense provided by the Vendor to the District under this provision must be free of any conflicts of interest, even if retention of separate legal counsel for the District is necessary. To the extent not inconsistent with the terms set forth in the underlying agreement between the parties, Vendor also agrees to defend, indemnify, and hold the District harmless for all costs, expenses, and attorneys' fees finally awarded by a court or that are included in a settlement entered into by the parties, directly resulting from Vendor's gross negligence or willful misconduct. The District agrees to notify the Vendor of such a claim within a reasonable time and agrees to cooperate with the Vendor in the defense and any related settlement.

#### **Section 5. OWNERSHIP OF DATA**

As between District and Vendor, the District retains ownership of all District Data provided to Vendor pursuant to the Parties' Agreement, regardless of whether such data is provided to Vendor by the District, its students, parents, guardians, or any other authorized user.

#### **Section 6. SECURITY BREACH REMEDIATION AND NOTICE**

6.1 Vendor agrees to maintain procedures and practices to preemptively safeguard against security breaches as described in KRS 61.932. However, in the event of a confirmed security breach as defined by KRS 61.931, Vendor shall notify the District within seventy-two (72) hours of confirmation of a security breach relating to the District Data in the possession of Vendor which compromises the security, confidentiality, or integrity of the District Data. The notification shall include, at a minimum, the following information to the extent known by the Vendor and as it becomes available: (a) the name and contact information of the individual reporting a breach to this section; (b) the date of the breach, or estimated date if not yet confirmed; (c) a list of the information and data reasonably believed

or confirmed to have been subject of the breach; (d) a list of the students whose information is believed to have been affected; and (e) a general description of the breach incident.

6.2 The Vendor further acknowledges and agrees to maintain a written incident response plan that reflects best practice and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incidents or unauthorized acquisition or use of confidential information and agrees to provide the District, upon request, with an overview of said written response plan.

6.3 In the event of a security breach relating to District Data or Personal Information in the possession of Vendor, Vendor shall bear the full cost of the notification and investigation requirements to the extent set forth in KRS 61.933.

6.4 In the event of a confirmed breach of District Data or Personal Information, as defined by KRS 61.931, Vendor agrees to retain an independent IT consulting firm and/or use it's own personnel and available resources, determined by the Vendor in it's exclusive discretion as reasonable and appropriate based on the severity of the breach, to provide requisite forensic/recovery/notification services consistent with and/or as provided for by the Commonwealth Office of Technology's recommended data breach response plan. Within 48 hours of completion of an applicable investigation, Vendor shall notify the District if the investigation finds that the misuse of District Data occurred or is likely to occur. Vendor shall additionally provide a copy of any investigation report rendered by the independent IT consulting firm insofar as the report relates to District Data, subject to appropriate confidentiality provisions. Finally, Vendor shall reimburse the District for the cost of notifying any impacted individuals of any such security breach, to the extent that notification to individuals by the District, and reimbursement by Vendor, is required by law.

6.5 Vendor agrees to adhere to applicable provisions of Kentucky Personal Information Security and Breach Investigation Procedure and Practices Act, KRS 61.932, *et seq.*

6.6 Vendor further agrees to adhere to all federal and state requirements pertaining to the prevention of, investigation of, response to, and remediation of any and all security breaches related to or unauthorized disclosures of District Data and PII.

6.7 In the event of a breach originating from the District's use of Vendor's Provided Services, Vendor shall reasonably cooperate with the District to the extent necessary to expeditiously secure any data subject to an unauthorized disclosure.

## **Section 7. CLOUD COMPUTING SERVICE PROVIDERS**

If the Vendor is a cloud computing service provider as defined in KRS 365.734(1)(b), Vendor agrees that:



- a. Vendor shall not process Confidential Student Information or any student data as defined by KRS 365.734 for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless Vendor receives express permission from the student's parent. Vendor shall work with the student's school and the District to determine the best method of collecting parental permission.
- b. Pursuant to KRS 365.734 (2), the Vendor shall not in any case process Confidential Student Information to advertise or facilitate advertising or to create or correct an individual or household profile for any advertising purpose and shall not sell, disclose, or otherwise process confidential student data for any commercial purpose;
- c. Pursuant to KRS 365.734 (3), the Vendor shall certify in writing to the District that it will comply with KRS 365.734(2).

**Section 8. NOTICES**

All notices or other communication required or permitted to be given pursuant to this agreement may be given via e-mail transmission or certified mail sent to the designated representatives below.

The designated representative for the District for this Agreement is:

Name: \_\_\_\_\_ Title: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 Phone: \_\_\_\_\_ Email \_\_\_\_\_

The designated representative for the Vendor for this Agreement is:

Name: \_\_\_\_\_ Charlie Lang \_\_\_\_\_ Title: \_\_\_\_\_ CPTO  
 Address: \_\_\_\_\_ 2201 Brookwood Dr., Little Rock, AR 72202  
 Phone: \_\_\_\_\_ 501-613-0370 \_\_\_\_\_ Email \_\_\_\_\_ privacy@apptegy.com

## **Section 9. Data Opt Out**

The District may provide a mechanism for students, parents, or guardians to opt out of any data sharing agreement with Vendor. In the event that a student, parent, or guardian opts out of any data sharing or Provided Services, the District shall notify Vendor of the opt-out within 48 hours of receipt. Within 48 hours of receipt of the opt-out notification and specific request for data deletion, Vendor shall delete any and all Confidential Student Information pertaining to that student, as well as his or her parent or guardian.

## **Section 10. MISCELLANEOUS PROVISIONS**

10.1 Open records. Vendor acknowledges that the District is subject to the Kentucky Open Records Act, KRS 61.870 to KRS 61.884 (“Open Records Act”), and may be required to disclose certain information obtained pursuant to the Parties’ relationship as set forth therein. Vendor agrees that it will not pursue any legal action against the District for any disclosure of Vendor’s information or data made in response to an Open Records Request. The District agrees to make reasonable efforts to claim all exemptions provided for in KRS 61.878 as appropriate and applicable to Vendor’s confidential and proprietary information.

10.2 Law enforcement or court-mandated disclosures. Should law enforcement or other government entities (“Requesting Part(ies)”) contact Vendor with a request for Confidential Student Data or District Data held by the Vendor pursuant any agreement of the Parties, the Vendor shall notify the District in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the District of the request. Similarly, if Vendor becomes legally compelled to disclose any District Data, Confidential Student Information, or Education Records (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), Vendor shall use all reasonable efforts to provide the District with advance notice before disclosure so that the District may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure the District’s compliance with the confidentiality requirement of federal or state law.

10.3 Equitable Relief. In any action or proceeding to enforce rights under the Agreement, the prevailing party will be entitled to recover reasonable costs and attorneys' fees if granted by a court of competent jurisdiction. The parties acknowledges that either party may seek and obtain injunctive relief for the unauthorized use or dissemination of District Data or Confidential Information, or other violations of the Parties’ Agreement, in addition to, and not in limitation of, other legal remedies provided under state and federal law.

10.4 Cooperation with District Auditor. The District has the right to annually audit (either internally or via a third party), upon written request, records of the Vendor directly relating to the performance of Provided Services as it pertains to Vendor’s data privacy processes

and procedures, subject to execution of appropriate confidentiality provisions including a confidentiality agreement. In the event of an annual audit, Vendor agrees to reasonably cooperate with District requests.

10.5 Severability. If any provision of this Agreement is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such invalidity, illegality, or unenforceability shall not affect the validity or enforceability of the remaining provisions of this Agreement. The parties agree that such invalid or unenforceable provision shall be modified to the extent necessary to make it valid, legal, and enforceable, and, to the greatest extent possible, that provision will be construed in a manner that reflects the original intent of the parties.


10.6 Successors Bound. This Agreement is and shall be binding upon the respective successors in interest to the Vendor in the event of a merger, acquisition, consolidation, or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this Agreement, the Provider shall ensure that any successor will assume the obligations of this Agreement and any obligations with respect to District Data within the underlying agreement between the parties. The Vendor shall provide written notice to the District no later than sixty (60) days after the closing date of sale, merger, or disposal. The District has the authority to review and address the Agreement if it disapproves of the successor to whom the Vendor is selling, merging, or otherwise disposing of its business.

10.7 Effect of Agreement. The Parties agree that the terms and conditions set forth in this Agreement modify, amend, or supplement any other agreement between the Parties and further agree to be bound to the terms herein. To the extent that the Agreement expressly conflicts with the terms and conditions of any other agreement between the Parties, this Agreement shall control.

[Remainder of this page intentionally left blank]

**IN WITNESS WHEREOF**, the District and Vendor execute this AGREEMENT to be effective and consistent with the effective date of the Parties' Agreement.

**BOONE COUNTY SCHOOL DISTRICT**

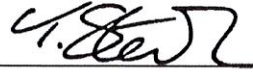
By:  SIGNATURE  
Kathleen Reutman

Printed Name: Name

Title/Position: Title/Position

Date: Date

**APPTEGY, INC.**

By:  \_\_\_\_\_

Printed Name: Tim Strudwick

Title/Position: CFO

Date: 2/12/2025

**Exhibit A: Products and Service**

This AGREEMENT covers access to and use of Apptey Inc's existing Provided Services that collect, process or transmit Student Data, as identified below:

Apptegy, Inc. owns and provides a software-as-a-service platform named Thrillshare. Using Thrillshare, clients can distribute communications and messaging across multiple outlets including an integrated website and mobile app. Thrillshare contains multiple features and functionality, including two primary components – Media and Rooms.

**CLIENT ADDENDUM TO MASTER SERVICES AGREEMENT  
BETWEEN BOONE COUNTY PUBLIC SCHOOLS  
AND APPTEGY**

The following is an addendum (“**Addendum**”) to the Master Services Agreement (“**Services Agreement**”) of Apptegy, Inc. (together with its affiliates, agents, and assigns, “**Apptegy**”) with the Boone County Public School District (“**School District**”). The effective date of the **Addendum** is the same as the **Services Agreement**.

This **Addendum** supplements and clarifies terms and provisions contained in the **Services Agreement**. In the event of a conflict or ambiguity with the terms and conditions of this **Addendum** and the **Services Agreement**, or any other agreement with Apptegy, the terms and conditions of this **Addendum** will control.

***WHEREFORE, BE IT AGREED TO BY THE PARTIES, AS AN ADDENDUM TO THE SERVICES AGREEMENT, AS FOLLOWS:***

1. Paragraph 1 of the Services Agreement (**Integration with Other Documents**) is hereby amended to provide that the Addendum and the Data Privacy and Security Agreement attached to this Addendum as Exhibit A are hereby expressly incorporated into, and integrated into the Services Agreement as if fully set forth therein. All other provisions of Paragraph 1 not inconsistent with this Addendum provision shall remain in effect.
2. Paragraph 2 of the Services Agreement (**Services; License**) shall be amended to provide that the license granted by Client to Apptegy shall be subject to the Data Privacy and Security Agreement attached to this Addendum as Exhibit A. All other provisions of Paragraph 2 not inconsistent with this Addendum provision shall remain in effect.
3. Notwithstanding any other provision of the Services Agreement, the Parties acknowledge and agree that as a political subdivision of the State of Kentucky, Client’s obligations to make payments under the Services Agreement is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. If funds are not appropriated or are otherwise legally unavailable to pay for any terms or renewals provided under the Services Agreement, Client may terminate the Services Agreement upon written notice to Apptegy, without further obligation, liability, or penalty. Client shall provide such notice as soon as reasonably practicable after it determines that sufficient funds will not be appropriated. In the event of such termination for non-appropriation of funds, Client shall not be liable for any future fees or penalties.
4. Paragraph 14 of the Services Agreement (**Miscellaneous**) is clarified to provide that the Agreement is governed at all times by the laws of the Commonwealth of Kentucky, without regard to conflict of law principles. The parties agree to submit to the exclusive jurisdiction and venue of the United States Federal District Court, Eastern District of Kentucky, at

Covington, Kentucky for any disputes relating to the Services or the Service Agreement, and/or Addendum, including Exhibit A.

5. The parties shall perform all of their obligations under the Services Agreement and the Addendum in accordance with the District's privacy policies governing student data and information under FERPA, and Exhibit A, the Data Privacy and Security Agreement, attached hereto and incorporated to this Addendum as if fully set forth herein.

IN WITNESS OF THIS AGREEMENT, the undersigned parties execute this Addendum to the Software and Services Agreement of Apptegy, effective as of the date set forth in the Services Agreement.

For Boone County Public Schools:

By: \_\_\_\_\_

Name: Jeff Hauswald, Superintendent

For Apptegy:

By: \_\_\_\_\_

Name: Tim Strudwick, CFO