

FOLLOW ALL PROCEDURES ON BACK OF THIS FORM

Contract # 250032
Number Assigned by Purchasing Dept.



CONTRACT REVIEW

BOARD MEETING DATE:

WHEN BOARD APPROVAL IS REQUIRED DO NOT PLACE ITEM ON AGENDA UNTIL REVIEW IS COMPLETED

Must Have Board Approval over \$100,000.00

Date Submitted: July 23, 2024

Name of Contract Initiator: Ethan Caren

Telephone #: ~~250032~~ 69603

School/Dept Submitting Contract: IT - 9040

Cost Center # 9040

Vendor Name: Apptegy

Contract Title: Apptegy

Contract Type: New Renewal Amendment Extension Previous Year Contract # ~~250032~~ 240176 & 210115

Contract Term: Annual *Subscription 7/1/2025 - 6/30/2026* Renewal Option(s): Annually - *Auto Renew 5% increase*

Contract Cost: \$348,250 (Renewal cost \$230,000 *annually*) + *5% annual renewal cost for the 1st year then Year cost +5% after that*

BUDGETED FUNDS – SEND CONTRACT PACKAGE DIRECTLY TO PURCHASING DEPT

Funding Source: Budget Line # 100.6500366.9040.0000.0000.0

Funding Source: Budget Line # _____

NO COST MASTER (COUNTY WIDE) CONTRACT - SEND CONTRACT PACKAGE DIRECTLY TO PURCHASING DEPT

INTERNAL ACCOUNT - IF FUNDED FROM SCHOOL IA FUNDS – SEND CONTRACT PACKAGE DIRECTLY TO SBAO

REQUIRED DOCUMENTS FOR CONTRACT REVIEW PACKAGE (when applicable):

xxx Completed Contract Review Form

____ SBAO Template Contract or other Contract (NOT SIGNED by District / School)

xxx SIGNED Addendum A (if not an SBAO Template Contract) - **When using the Addendum A, this Statement MUST BE included in the body of the Contract:**

“The terms and conditions of Addendum A are hereby incorporated into this Agreement and the same shall govern and prevail over any conflicting terms and/or conditions herein stated.”

xxx Certificate of Insurance (COI) for General Liability & Workers’ Compensation that meet these requirements:

COI must list the School Board of Clay County, Florida as an Additional Insured and Certificate Holder. Insurer must be rated as A- or better.

General Liability = \$1,000,000 Each Occurrence & \$2,000,000 General Aggregate.

Auto Liability = \$1,000,000 Combined Single Limit (\$5,000,000 for Charter Buses).

Workers’ Compensation = \$100,000 Minimum

[If exempt from Workers’ Compensation Insurance, vendor/contractor must sign a Release and Hold Harmless Form. If not exempt, vendor/contractor must provide Workers’ Compensation coverage].

____ State of Florida Workers Comp Exemption (<https://apps.fldfs.com/bocexempt/>) (If Applicable)

____ Release and Hold Harmless (If Applicable)

RECEIVED

By Elaine at 2:39 pm, Aug 06, 2024

****AREA BELOW FOR DISTRICT PERSONNEL ONLY ****

CONTRACT REVIEWED BY:	COMMENTS BELOW BY REVIEWING DEPARTMENT
Purchasing Department 	TIPS Contract 230105 / FLDOE 6A-1.012 (14) Information Technology <i>See Order form for clarification on Initial Term, Annual Renewal & Pricing</i>
School Board Attorney JPS Review Date: 8/23	<i>Vendor requests changes to SBCC Addendum A so defer approval to Attorney</i> <i>Changes to Addendum A are okay. Approved.</i>
Other Dept. as Necessary Review Date	SBCC Data Share Agreement Attached
PENDING STATUS: <input type="checkbox"/> YES <input type="checkbox"/> NO	IF YES, HIGHLIGHTED COMMENTS ABOVE MUST BE CORRECTED BY INITIATOR
FINAL STATUS	

CONTRACT REVIEW PROCESS FOR "ALL" CONTRACTS

A contract is defined as an agreement between two or more parties that is intended to have legal effect. This may include MOUs, Interlocal Agreements, Service Agreements and Contracts. Contracts document the mutual understanding between the parties as to the terms and conditions of their agreement, contain mutual obligations, and clearly state the agreement's consideration. The term consideration includes the cost of the services and/or products to be provided by second party (vendor or service provider) and any non-monetary performance. No school, department, or other organizational unit has authority to contract in its own name. All Board contracts must be made in the legal name of the Board, "The School Board of Clay County, Florida". The School or Department may extend this name to include the school or department as follows, "The School Board of Clay County, Florida o/b/o _____ (insert the school or department name)" where o/b/o means "on behalf of".

All contracts shall be reviewed and approved by the School Board Attorney and/or the Supervisor of Purchasing to ensure legality, compliance with Board policy, and to ensure the Board interests are protected before the authorized signatory may execute the contract.

All contracts having a value of \$100,000 or more shall be authorized by the Board at a regular or special meeting and signed by the Board Chairman. All approved contracts having a value of less than \$100,000 may be executed by the Superintendent or appropriate District administrator based on the value of the contract.

1. All approved contracts having a value of \$50,000 or more, but less than \$100,000 shall be signed by the Superintendent, or the person who has been designated, in writing by the Superintendent, as the Superintendent's Designee at the time of the contract signing. All contracts executed pursuant to this subparagraph shall be reported to the School Board in a separate entry as part of the monthly financial report.
2. All approved contracts having a value of \$25,000 or more, but less than \$50,000, shall be signed by the Superintendent, or the Assistant Superintendent for Business Affairs.
3. All approved contracts having a value of less than \$25,000 and contracts of any value described in Board Authorized Contracts above that are exempt from the requirement for Board approval, may be signed by the Superintendent, or the Assistant Superintendent for their Division, or Chief Officers, or Directors, or Principals.
4. The Superintendent is authorized to approve contract amendments or change orders for the purchase of commodities and services up to the amount of ten (10) percent or \$50,000, whichever is less, of the original contract amount that was previously approved by the Board.

Employees who enter into agreements without authority may be personally liable for such agreements, whether oral or written.

Step 1: Contract Initiator and Vendor prepare draft contract
(School Board Attorney Office (SBAO) Template Contracts available on SBAO webpage are strongly encouraged)

Step 2: Complete Contract Review Form, attach Required Documents to include the UNSIGNED Contract by the District / School.

For Contracts using Budgeted Funds or For No Cost / Master (County Wide) Contracts:
Initiator submits Contract Review Package to Purchasing Department - See Step 3

For Contracts using Internal Funds Individual to each School:
Initiator submits Contract Review Package direct to SBAO - See Step 4

IMPORTANT

Step 3: If Funded by Budgeted Funds, submit the Contract Review Package to the Purchasing Department. Purchasing will begin the contract review process and submit the contract to the SBAO for review. SBAO may reach out to Initiator and/or other Departments (Risk, IT,) with questions or concerns and will assist with contract revisions. SBAO will send the Contract Review Package back to the Purchasing Department for final processing and the return to Initiator.

Purchasing will log "District" Contracts (Cost/No Cost) on Contract Review Log and save copy of the Contract Review Package PLUS the Final Signed Contract you've return to Purchasing in the Contract Review Team Drive.

Step 4: If Funded by Internal Account (IA), submit the Contract Review Package directly to SBAO.
Email: contractreview@myoneclay.net
The SBAO will begin the contract review process and return it directly to Initiator

Step 5: The Initiator is responsible for finalizing the Contract which includes:
Addressing Comments/Revisions, Obtaining Required Signatures, Send District Final Signed Contract to Purchasing OR Retain Internal Accounts Final Signed Contract at School per School Board Record Policy.
If there is a Cost associated with Contract, the Initiator must work with their Bookkeeper to finalize the Purchasing Process.
Budgeted Funds require a District Purchase Order. Internal Accounts require an IA Purchase Order.

For assistance with legal-related matters, please visit the [School Board Attorney's Office \("SBAO"\) webpage](#) or call 904-336-6507
For assistance with insurance-related matters, please visit the [Business Affairs - Risk Management webpage](#) or call 904-336-6745
For assistance with District Purchasing, please visit the [Business Affairs - Purchasing webpage](#) or call 904-336-6736



Order Form

Client Name: School District of Clay County, FL			
Address: 900 Walnut St, Green Cove Springs		Email: ashley.gilhousen@myoneclay.net	
Florida 32043		Phone: 9043366500	
Description	Price	Qty	Subtotal
Mobile App Development (one-time) One-time app development for iOS and Android apps for the District + 43 campuses	\$31,000	1	\$31,000
Rooms Development (one-time) Rostering of all classes, teams, etc.	\$19,000	1	\$19,000
Thrillshare Media (6-months prorated) Thrillshare Publishing Platform (desktop and mobile) for ~40,000 students	\$68,250	1	\$68,250
Thrillshare Media (annual) Thrillshare Publishing Platform (desktop and mobile) for ~40,000 students	\$136,500	1	\$136,500
Rooms (annual) Thrillshare Rooms Publishing Platform (desktop and mobile) for ~40,000 students	\$93,500	1	\$93,500
Website design and hosting Up to 1 re-design per contract year Included in Thrillshare Media cost	\$0	1	\$0
Alerts Unlimited text, voice, and email alerts Included in Thrillshare Media 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
Support, service, and training Included in Thrillshare Media and Rooms cost	\$0	1	\$0
Static content migration Included in Thrillshare Media cost	\$0	1	\$0

Annual line items are 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).



Payment Schedule

Payment Schedule: Payable subject to the terms of Agreement	Amount
Total of the above, collectively, the "Services"	\$348,250.00
Billed after signature	\$31,000 - Thrillshare Media development cost
January 1, 2025 ("Client Start Date" for Thrillshare Media)	\$68,250 - Thrillshare Media 6-months prorated - Term 1/1/25–6/30/25 \$19,000 - Rooms development cost
July 1, 2025 ("Client Start Date" for Rooms)	\$230,000 - Thrillshare Media (\$136,500) and Rooms (\$93,500) annual cost - Term 7/1/25–6/30/26
July 1, 2026 (if renewed)	if renewed: \$241,500 - Thrillshare Media (\$143,325) and Rooms (\$98,175) annual cost - Term 7/1/25–6/30/26 *Includes 5% increase for renewal

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") and the attached Addendum A ("Client Addendum"). 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

Apptegy, Inc.

By:  SIGNATURE
Ashley Gilhousen

By:  SIGNATURE
Matthias Wehnert

Name: Ashley Gilhousen

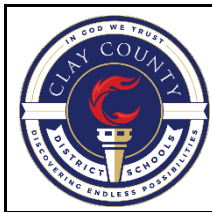
Name: Matthias Wehnert

Title: Board Chairperson

Title: VP of Enterprise Sales

Date:

This contract is in line with TIPS contract #230105



"ADDENDUM A" TO CONTRACT WITH THE SCHOOL BOARD OF CLAY COUNTY, FLORIDA AND APPTEGY

Notwithstanding any contractual language to the contrary, the terms and conditions of this "Addendum A" shall govern and prevail over any conflicting or inconsistent terms and conditions in the underlying contract to which this "Addendum A" is attached and/or otherwise incorporated. For clarity, the underlying contract consists of the Order Form, payment Schedule, Master Services Agreement, Terms of Use, and Privacy Policy (as amended from time to time and found at www.apptegy.com/terms-of-use and www.apptegy.com/privacy) (collectively, the "Master Services Agreement"). All references herein made to the School Board of Clay County, Florida ("SBCC") shall be interpreted to include the School Board of Clay County, Florida, Clay County District Schools ("District"), and all Board officers and employees.

1. The Company, Vendor, Agency, or Consultant, of Contract with the School Board of Clay County, hereafter collectively and individually referred to as the "CONTRACTOR".
2. CONTRACTOR represents that it is an independent contractor and that it requires that the SBCC treat it as such. CONTRACTOR agrees:
 - a. That it has no rights to any benefits extended by the SBCC to its employees [including without limitation, sick leave, vacation time, insurance coverage, etc.];
 - b. That it will not take a position contrary to their status as an independent contractor, and agrees to accept the responsibilities placed on independent contractors by federal and state law accordingly, the SBCC will not make the deductions or contributions that an employer may be required to make with respect to its employees, and the undersigned will be responsible for all federal and state tax and fund obligations, including without limitation, income tax, Social Security, unemployment compensation, etc.];
 - c. CONTRACTOR agrees, as an independent contractor and not an employee of the SBCC, it is responsible for providing their own Worker's Compensation Insurance and social security/self-employment contributions.
3. CONTRACTOR shall indemnify, defend, and hold harmless the SBCC, its officers, and employees from any claim, loss, damage, penalty, or liability arising from the gross negligence or intentional misconduct of CONTRACTOR, its employees, or agents relating to the performance of duties imposed upon CONTRACTOR by this Agreement. Such indemnity shall not be limited by benefits payable by or for CONTRACTOR under worker's compensation, disability, or any other employee benefits or insurance programs or policies. Contractor shall timely provide to the SBCC written notice of any claim, complaint, or demand asserted against CONTRACTOR related to the performance of this Agreement. CONTRACTOR's obligations under this section shall survive the termination of this Agreement.
4. CONTRACTOR agrees to be bound by, and at its own expense comply with, all federal, state, and local laws, ordinances, and regulations applicable to the services. CONTRACTOR shall review and comply with the confidentiality requirements of federal and state law regarding access to and use of records. CONTRACTOR agrees to use industry-accepted, administrative, physical, and technical safeguards to help ensure the privacy of these records and will use the information in the records it receives only for the purpose of providing the services.
5. Reservation of Sovereign Immunity: No provision or language in the underlying contract shall be construed or interpreted to increase the scope or dollar limit of the SBCC's liability beyond that which is set forth in Section 768.28 of the Florida Statutes. Nor shall any such language be construed or interpreted to waive the SBCC's sovereign immunity from suit, or to require the SBCC to indemnify CONTRACTOR or any other person, corporation or legal entity of any kind or nature whatsoever for injury or loss resulting from any acts or omissions other than those which arise from the actionable negligence of the SBCC. The SBCC expressly reserves all other protections and privileges related to its sovereign immunity.
6. CONTRACTOR warrants that any services provided under this agreement will be performed in a workmanlike manner, in accordance with the standard of care, skill, training, diligence, and judgement provided by competent providers performing services of a similar nature. In the event of the unavailability of the services, SBCC's remedies will be as provided for in CONTRACTOR's standard Service Level Agreement, attached hereto and incorporated herein.

7. Method of Payment (if applicable): Services and/or Products satisfactorily received shall be compensated in accordance with Attachment A, CONTRACTOR's Master Services Agreement, including Order Form and Payment Schedule, and the following terms:
 - a. Procurement is performed in accordance with applicable law, State Board of Education Rules, Clay County School Board Policy and other applicable rules and regulations which govern. CONTRACTOR shall be paid in accordance with CONTRACTOR's Order Form and Payment Schedule, the Local Government Prompt Payment Act (218.70, et seq., Florida Statutes) as applicable, and upon submission of detailed invoices to the appropriate location listed on the District Purchase Order and/or the School Internal Account Purchase Order.
 - b. Unless otherwise required by law, the SBCC's payment obligations (if any) arising from the underlying Agreement are contingent upon an annual appropriation by the School Board and the availability of funds to pay for the contracted services and/or products provided. If such funds are not appropriated for the underlying Agreement and results in its termination, such conditions/events shall not constitute a default by the SBCC.
8. If it is determined by the SBCC that the work is not being performed as agreed herein, CONTRACTOR shall be deemed to be in default, and the SBCC reserves the right to cancel this Agreement immediately for cause. Notwithstanding the foregoing, all fees paid to CONTRACTOR are nonrefundable, subject only to applicable procurement and appropriations law.
9. Force Majeure: Neither party to this Agreement shall be liable for delays or failures in performance under this Agreement (other than obligations relating to payment, confidentiality, and protection of ownership and intellectual property rights) resulting from acts or events beyond the reasonable control of such party (a "Force Majeure Event"), including acts of war, terrorism, acts of God, earthquake, flood, embargo, riot, sabotage, labor dispute, wide spread outbreak of disease or pandemic, governmental act, failure of the internet, power failure, or energy, utility, or telecommunications interruptions, provided that the delayed party: (i) gives the other party prompt notice of such cause; and (ii) uses its reasonable commercial efforts to promptly correct such failure or delay in performance. In the event that a Force Majeure Event lasts for more than 90 days, and the party experiencing the initial delay cannot correct its failure or delay in performance during that period of time, despite using its reasonable commercial efforts to do so, the other party may terminate the affected portions of this Agreement.
10. This Agreement shall not be modified or amended except in writing, duly agreed to and executed by the parties.
11. Except in connection with a merger, acquisition, or sale of all or substantially all of a party's assets or voting securities, CONTRACTOR shall not assign this Agreement in whole or in part, without the express written consent of the SBCC Purchasing Department.
12. This Agreement shall be governed by and construed in accordance with the laws of the State of Florida and venue shall be in Clay County, Florida.
13. No other representations or promises shall be binding on the parties hereto except those representations or promises contained herein.
14. In the event that any part, term, or provision of this Agreement is, in a court of competent jurisdiction, found to be illegal or unenforceable, the validity of the remaining portions and provisions will not be affected, and the rights and obligations of the parties shall be construed and enforced as if this Agreement did not contain the particular part, term, or provision held to be so invalid.
15. Should any litigation be commenced in connection with this Agreement, the prevailing party shall be entitled to reasonable attorney fees and court costs.
16. The parties hereto represent that they have reviewed this Agreement and have sought legal advice concerning the legal significance and ramifications of this Agreement.
17. CONTRACTOR shall retain records associated with the services and/or products provided herein for a period of three years following final payment. CONTRACTOR shall, with reasonable notice, provide the SBCC access to these records during the above retention period.
18. Jessica Lunsford Act: SBCC is required to conduct background screening of CONTRACTOR (including its employees, agents, and sub-contractors) (go to [Clay County District Schools website](#) for fingerprinting procedures). CONTRACTOR represents and warrants to the SBCC that CONTRACTOR is familiar with Sections 1012.32,

1012.321, 1012.465, 1012.467, and 1012.468 of the Florida Statutes regarding background investigations. CONTRACTOR covenants to comply with all requirements of the above-cited statutes at CONTRACTOR's sole expense and shall provide the SBCC proof of such compliance upon request.

Certification: By executing this Agreement, CONTRACTOR swears and affirms under penalty of perjury that all of its employees and; agents, will comply with these procedures, the requirements of the Jessica Lunsford Act, SBCC's finger printing procedures, and the laws of the State of Florida. Failure to comply with these procedures, the Act, SBCC's finger printing procedures, and the law of the State of Florida shall constitute a material breach of the Agreement, and SBCC may avail itself of all remedies pursuant to law. CONTRACTOR agrees to indemnify and hold harmless SBCC, its officers, employees, and agents, from and against any and all claims or causes of action, including without limitation those for personal injury, death, property damages, and attorney fees, arising out of or relating to CONTRACTOR's failure to comply with any of the above.

19. E-Verify: CONTRACTOR named herein, is required to register with and use the U.S. Department of Homeland Security's (DHS) E-Verify system to verify the work authorization status of all newly hired employees. By executing this Agreement, the CONTRACTOR certifies that it is, registered with, and use, the E-Verify system for all newly hired employees. The CONTRACTOR must maintain a copy of such affidavit for the duration of the Agreement. This section serves as notice to the CONTRACTOR that, pursuant to the terms of Section 448.095(2)(c) 1 and 2, Florida Statutes, the SBCC shall terminate this Agreement if it has a good faith belief that the CONTRACTOR has knowingly violated Section 448.09(1), F.S. If the SBCC terminates an Agreement with a CONTRACTOR pursuant to sec. 448.095(2)(c), F.S., the CONTRACTOR will not be awarded a public contract for at least one year after the date of such termination.
20. The CONTRACTOR certifies that CONTRACTOR is in compliance with the requirements of law regarding equal employment opportunity for all persons without regard to age, race, color, religion, sex, national origin, or disability and is not on the Discriminatory Vendor List pursuant to Florida Statute 287.134.
21. CONTRACTOR shall, at CONTRACTOR's sole expense, procure and maintain during the term of this Agreement, at least the following minimum insurance coverage, which shall not limit the liability of CONTRACTOR:

<u>General Liability Policy:</u>	<u>Auto Liability Policy:</u>	<u>Worker's Compensation Policy:</u>
\$1,000,000.00 per occurrence	\$1,000,000.00 combined single limit	\$100,000
\$2,000,000.00 aggregate		<i>*Exempt, need signed WCAF</i>

**If the CONTRACTOR is exempt from Worker's Compensation insurance obligations, the CONTRACTOR must sign the Worker's Compensation Acknowledgment Form (WCAF) attached hereto as Exhibit # 1.*

All policies of insurance shall be rated "A-" or better by the most recently published A.M. Best Rating Guide and shall be subject to the SBCC approval as to form and issuing company. The SBCC shall be named as certificate holder and as an *additional insured* in the comprehensive general (including property damage) liability policy by means of blanket additional insured clause. Upon SBCC's request, CONTRACTOR shall furnish the SBCC's Representative copies of insurance certificates evidencing that it maintains at least the insurance coverage required hereunder. CONTRACTOR is NOT authorized to proceed with the services until all the insurance certificates have been received and accepted, such acceptance not to be unreasonable withheld.

Receipt of certificates or other documentation of insurance or policies or copies of policies by the SBCC, or by any of its representatives, which indicate less coverage than required does not constitute a waiver of CONTRACTOR's obligation to fulfill the insurance requirements herein.

22. CONTRACTOR shall not solicit or accept brokerage or any other fees or remuneration from any provider of the SBCC insurance program.
23. CONTRACTOR recognizes and acknowledges that by virtue of entering into this Agreement and providing services hereunder, CONTRACTOR, its agents, employees, and officers, may have access to certain confidential information and processes, including confidential student information, and financial records, (hereinafter "Confidential Information"). CONTRACTOR agrees that neither it nor any CONTRACTOR agent, employee, or officer, will at any time, either during or subsequent to the term of this Agreement, disclose to any third party, except to the extent necessary for CONTRACTOR to provide its services to SBCC, where permitted or required by law or where such disclosure is expressly approved by the SBCC in writing, any Confidential Information. In addition, following

expiration of said Agreement and upon request by SBCC, CONTRACTOR, its agents, employees, or officers; shall either destroy or return to the SBCC all Confidential Information stored by CONTRACTOR. With 72-hours written notification from CONTRACTOR that data has been destroyed or returned, the SBCC reserves the right to determine whether or not Confidential Information has been destroyed and such confirmation may include inspecting the CONTRACTOR's facilities and equipment. Notwithstanding the foregoing, any right by SBCC to inspect or audit CONTRACTOR's facilities or equipment shall be limited in scope to the extent commercially reasonable, and shall be at the sole expense of SBCC. CONTRACTOR understands and agrees that it is subject to all federal and state laws and SBCC rules relating to the confidentiality of student information. Contractor further agrees to comply with the Family Educational Rights and Privacy Act ("FERPA") 34 C.F.R. § 99. Contractor shall regard all student information as confidential and will not disclose personally-identifiable student records or information to any third party without appropriate legal authorization. Access to SBCC data or networks shall require a SBCC Data-Sharing and Usage Agreement and shall only be authorized by the SBCC IT Department.

24. For clarity, CONTRACTOR only collects, uses, and maintains SBCC's data under the direct control of SBCC. Notwithstanding the foregoing, CONTRACTOR acknowledges and agrees that SBCC is subject to and must comply with Florida's Public Records law. Upon request, CONTRACTOR will provide SBCC with copies of SBCC's data stored by CONTRACTOR. If a public records request for SBCC's information is submitted to and received by CONTRACTOR, CONTRACTOR will use commercially reasonable efforts to promptly notify SBCC of the request and, at SBCC's direction, help assist SBCC in responding to the request (including, as indicated, by providing SBCC copies of SBCC's data stored by CONTRACTOR). Additionally, if, and only to the extent, required by CONTRACTOR under 119.0701, Florida Statutes or other provisions of the Public Records law, CONTRACTOR shall:
- Keep, maintain, and produce upon request and within a reasonable period of time all data created or collected in the performance of its duties under this Agreement ("Agreement Data") which come within the definition of a "public record" under Chapter 119.
 - Provide to the SBCC, upon its request and free of charge, a copy of each record which CONTRACTOR seeks to produce in response to a public records request.
 - Ensure that all Agreement Data considered exempt under Chapter 119 are not disclosed except as authorized by law.
 - Upon completion of its obligations under the Agreement, transfer to the SBCC, at no cost, all Agreement Data in CONTRACTOR's possession or otherwise keep and maintain such data/records as required by law. All records transmitted to the SBCC must be provided in a format that is compatible the SBCC's information technology systems.

CONTRACTOR's failure to comply with the provisions set forth in this section shall constitute a default and material breach of this Agreement, which may result in termination by the SBCC without penalty.

IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, OR CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTRACTOR SHALL CONTACT THE SBCC'S CUSTODIAN OF PUBLIC RECORDS AT 900 WALNUT STREET, GREEN COVE SPRINGS, FLORIDA 32043, OR AT 904-336-6500, OR AT: PRR@myoneclay.net

25. Government Funding (if Applicable): Funding for this Agreement may be provided in whole or in part by one or more Government funding agencies (Federal, State, Local). As a result, CONTRACTOR shall comply with applicable Laws, Regulations, Executive Orders, and Governmental Agency Rules and Policies included but not limited to Titles: 2 – Grants and Agreements (2 C.F.R. §200), Title 7 – Agriculture (NSLP), Title 34 – Education (EDGAR, FERPA), Title 44 – Emergency Management and Assistance (FEMA); U.S. Code Titles: 20,31,40,41. To the extent that the SBCC is using Government Funds as a source of payment for this Agreement, CONTRACTOR shall execute and deliver to the SBCC the following forms, attached hereto as Exhibit # 2: (a) EDGAR Certification; (b) Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion; (c) Drug-Free Workplace Certification; (d) Non-Collusion Affidavit; and (e) Disclosure of Potential Conflict of Interest.

SBCC'S Representative with CONTRACTOR is: _____

School/Department Name: _____

Mailing Address: _____

Phone #: _____ Email Address: _____

Accepted and Agreed to:

SCHOOL BOARD OF CLAY COUNTY

CONTRACTOR

By: _____

By: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Exhibit # 1

WORKERS COMPENSATION ACKNOWLEDGEMENT FORM (WCAF)

The undersigned Contractor/Vendor (“Contractor”) represents and acknowledges that it is an independent contractor and is not provided coverage under any self-insured workers compensation program of the School Board of Clay County, Florida (the “Board” or “District”), any primary workers compensation insurance policy purchased by or on behalf of the District, any excess workers compensation insurance purchased by or on behalf of the District, any risk sharing arrangement, risk sharing pool, or any state reimbursement fund for workers compensation payments made by the District, based on the following understandings and representations by the Contractor:

1. Contractor is not an “Employee” as defined under Chapter 440 of the Florida Statutes. The Parties agree that Chapter 440 describes remedies for employers and employees in place of Florida common law and limits the rights of independent contractors like the undersigned.
2. Contractor maintains a separate business with its own work equipment, material, and accommodations.
3. Contractor has a different federal employer identification number than the District or is a sole proprietor who is not required to obtain a federal employer identification number under state or federal regulations.
4. Contractor receives compensation for services rendered or work performed, and such compensation is paid to a business rather than to an individual.
5. Contractor maintains at least one bank account in the name of the Contractor or associated persons or entities for the purposes of paying business expenses related to the services rendered or work performed for the District.
6. Contractor performs work or is able to perform work for entities other than the District at the Contractor’s election without the necessity of completing an employment application or process.
7. Contractor either provides its own workers compensation coverage or has elected to be exempt from workers compensation coverage.
8. Contractor has provided proof of other insurance, including liability insurance, to the District in the amounts required by the District.
9. Contractor had an opportunity to review and consult with legal counsel regarding this document.
10. Contractor understands that the District is relying upon the truthfulness and accuracy of representations in this acknowledgement as a material basis for the District entering into the underlying agreement(s) with Contractor.

Name of Contractor/Vendor: _____

Signature of Authorized Representative: _____

Printed Name of Authorized Representative: _____

Title of Authorized Representative: _____

Date: _____

Exhibit # 2 (a)

EDGAR CERTIFICATIONS

All purchases involving the expenditure of federal funds must be compliant with the Education Department General Administrative Regulations ("EDGAR"). The following certifications and provisions are required and apply when the School Board of Clay County, Florida ("SBCC" "School Board") expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the District shall contain the procurement provisions of Appendix II to Part 200, as applicable.

REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS APPENDIX II to C.F.R. PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at \$150,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Pursuant to Federal Rule (A) above, when School Board expends federal funds, School Board reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

(B) All contracts in excess of \$10,000 must address termination for cause and for convenience by the non-Federal entity including the manner by which it will be effected and the basis for settlement.

Pursuant to Federal Rule (B) above, for all contracts involving Federal funds in excess of \$10,000, School Board reserves the right to terminate the contract (i) for convenience, and/or (ii) for cause by issuing a certified notice to the vendor.

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to Federal Rule (C) above, when School Board expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

Pursuant to Federal Rule (D) above, when School Board expends federal funds during the term of an award for all contracts and subgrants for construction or repair, Vendor will be in compliance with all applicable Davis-Bacon Act provisions.

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29

EDGAR CERTIFICATIONS (continued)

CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Pursuant to Federal Rule (E) above, when federal funds are expended by School Board, Vendor certifies that Vendor will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award resulting from this procurement process.

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of “funding agreement” under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

Pursuant to Federal Rule (F) above, when federal funds are expended by School Board, Vendor certifies that Vendor will be in compliance with all applicable provisions of Federal Rule (F) during the term of an award resulting from this procurement process.

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401 7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

Pursuant to Federal Rule (G) above, when federal funds are expended by School Board, Vendor certifies that Vendor will be in compliance with all applicable provisions of Federal Rule (G) during the term of an award resulting from this procurement process.

(H) Energy Policy and Conservation Act (2 CFR §910.120, 10 CFR §600.236). Vendor agrees to comply with the mandatory standards and policies relating to energy efficiency contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act.

Pursuant to Federal Rule (H) above, when federal funds are expended by School Board, Vendor certifies that Vendor will be in compliance with all applicable provisions of Federal Rule (H) during the term of an award resulting from this procurement process.

(I) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to Federal Rule (I) above, when federal funds are expended by School Board, Vendor certifies that during the term of an award resulting from this procurement process, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency.

(J) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

Pursuant to Federal Rule (J) above, Vendor certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The Vendor further certifies that: (1) No Federal appropriated funds have been

EDGAR CERTIFICATIONS (continued)

paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement. (2) If any funds other than Federal appropriated funds have been paid to any person for influencing or attempting to influence an officer or employee of any agency, Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions. (3) The undersigned shall require that the language of this certification be included in the award documents for all covered subawards in Federal funds at all appropriate tiers and that all subrecipients shall certify and disclose accordingly.

RECORDS ACCESS AND RETENTION

Records Access (34 CFR 80.36 (i)(10): All vendors, contracts and subcontractors shall give access to the SBCC, the appropriate Federal agency, the Comptroller General of the United States, or any of their duly authorized representative to any books, documents, papers, and records of the vendor which are directly pertinent to this specific bid/contract for the purpose of making audit, examination, excerpts and transcriptions.

Records Retention (2 C.F.R. § 200.333): Financial records, supporting documents, statistical records and all other non-Federal entity records pertinent to a Federal award must be retained for a period of three (3) years from the date of submission of the final expenditure report or, for Federal awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, respectively, as reported to the Federal awarding agency or passthrough entity in the case of a subrecipient.

RECOVERED MATERIALS

Recovered Materials (2 CFR §200.322): Contractor must comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

Vendor agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that vendor certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above.

Vendor's Name: _____

Signature of Authorized Representative: _____

Print Name of Authorized Representative: _____

Exhibit # 2 (b)

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION - LOWER TIER COVERED TRANSACTIONS

This certification is required by the Department of Education regulations implementing Executive Order 12549, Debarment and Suspension, 34 CFR Part 85, for all lower tier transactions meeting the threshold and tier requirements stated at Section 85.110.

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.
2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.
3. The prospective lower tier participant shall provide immediate written notice to the person to whom this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
4. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.
5. The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.
6. The prospective lower tier participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion - Lower Tier Covered Transactions," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Non-Procurement List.
8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Instructions for Certification:

1. The prospective lower tier participant certifies, by submission of this proposal that neither it nor its principals are:
 - a) presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency;
 - b) have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in performing a public (federal, state or local) transaction or contract under a public transaction; or for violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property;
 - c) are not presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of the offenses enumerated in this certification; or
 - d) have not within a three-year period preceding this application had one or more public transaction (federal, state or local) terminated for cause or default.
2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Name of Vendor: _____

Printed Name

Title of Authorized Representative

Signature: _____

Date: _____

Exhibit # 2 (c)

DRUG-FREE WORKPLACE CERTIFICATION

Preference shall be given to vendors/contractors certifying their compliance with a drug-free workplace in accordance with Section 287.087, Florida Stat. as follows:

Preference to businesses with drug-free workplace programs - Whenever two or more bids, proposals, or replies that are equal with respect to price, quality, and service, are received by the State or by any political subdivision for the procurement of commodities or contractual services, a bid, proposal, or reply received from a business that certifies that it has implemented a drug-free workplace program shall be given preference in the award process. Established procedures for processing tied bids, proposal, or replies shall be followed if none of the tied vendor has a drug-free workplace program. In order to have a drug-free workplace program, a business shall:

1. Publish a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the workplace and specifying the actions what shall be taken against employee for violations of such prohibition.
2. Inform employees about the dangers of drug abuse in the workplace, the business’s policy of maintaining a drug-free workplace, any available drug counseling, rehabilitation, and employee assistance programs, and the penalties that may be imposed upon employees for drug abuse violations.
3. Give each employee engaged in providing the commodities or contractual services that are under bid a copy of the statement specified in subsection (1).
4. In the statement specified in subsection (1), notify the employees that, as a condition of working on the commodities or contractual services that are under bid, the employee shall abide by the terms of the statement and shall notify the employer of any conviction of, or plea of guilty or nolo contendere to, any violation of Chapter 893 or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction.
5. Impose a sanction on, or require the satisfactory participation in a drug abuse assistance or rehabilitation program if such is available in the employee’s community, by any employee who is so convicted.
6. Make a good faith effort to continue to maintain a drug-free workplace through implementation of this section.

As the person authorized to sign the statement, I certify that this firm complies fully with the above requirements.

CONTRACTOR NAME: _____

AUTHORIZED CONTRACTOR REPRESENTATIVE SIGNATURE:

(Printed Name)

(Signature)

(Title)

(Date)

Exhibit # 2 (d)

NON-COLLUSION AFFIDAVIT

State of FLORIDA)
County of CLAY)

My name is (INSERT NAME _____). I hereby attest that I am authorized to execute this affidavit on behalf of my firm, its owners, directors, and officers. I have personal knowledge of the price(s), guarantees and the total financial commitment represented in the firm's offer and/or contract.

(1) The firm's prices and amounts offered have been arrived at independently and without consultation, communication or agreement with any other contractor or respondent.

(2) Neither the final nor approximate prices or amounts offered have been disclosed to any other firm or person who is a respondent or potential respondent, nor were they disclosed prior to opening of offers.

(3) The offer from my firm is made in good faith and no attempt has been made to induce any firm or person to refrain from submitting an offer, or to submit an offer higher than our offer, or to submit any intentionally high or noncompetitive offer or other form of complementary offer.

(4) (INSERT NAME OF COMPANY _____) its affiliates, subsidiaries, officers, directors, employees are not currently under investigation by any governmental agency and have not in the last three years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding, proposing or offering on any public contract, except as follows:

I attest that (INSERT NAME OF COMPANY _____) understands and acknowledges that the above representations are material and important, and will be relied on by The School Board of Clay County, Florida, in awarding the contract for which this offer is submitted. I understand and my firm understands that any misstatement of material representations herein shall be treated as fraudulent or otherwise intentional concealment of the true facts relating to submission of offers for this contract.

CONTRACTOR NAME: _____

AUTHORIZED CONTACTOR REPRESENTATIVE SIGNATURE:

(Printed Name)

(Signature)

(Title)

(Date)

Exhibit # 2 (e)

**DISCLOSURE OF POTENTIAL CONFLICT OF INTEREST AND
CONFLICTING EMPLOYMENT OR CONTRACTUAL RELATIONSHIP**

Section 112.313 (3) and (7), Florida Statutes, sets forth restrictions on the ability of SBCC employees acting in a private capacity to rent, lease, or sell any realty, goods or services to SBCC. It also places restrictions on SBCC employees concerning outside employment or contractual relationships with any business entity which is doing business with SBCC.

Contractor must disclose the names of any employees who are employed by Contractor who are also an employees of SBCC. Persons identified below may have obligations and restrictions applicable to them under Chapter 112, Florida Statutes.

Name of Contractor's Employee	SBCC Title or Position of Contractor's Employee	SBCC Department/School of Contractor's Employee
_____	_____	_____
_____	_____	_____
_____	_____	_____

Check one of the following and sign:

I hereby affirm that there are no known persons employed by Contractor who are also an employee of SBCC.

I hereby affirm that all known persons who are employed by Contractor who are also an employee of SBCC have been identified above.

Signature

Company Name

Exhibit # 2 (f)

STATE OF FLORIDA REQUIRED AFFIDAVITS

FOREIGN COUNTRY OF CONCERN ATTESTATION

Form must be completed by an officer or representative of an entity submitting a bid, proposal, reply to, entering into, renewing, or extending, a contract with a Governmental Entity which would grant the entity access to an individual's Personal Identifying Information. Capitalized terms used herein have definitions ascribed in Rule [60A-1.020, F.A.C.](#)

(INSERT NAME OF COMPANY _____) is not owned by the government of a Foreign Country of Concern, is not organized under the laws of nor has its Principal Place of Business in a Foreign Country of Concern, and the government of a Foreign Country of Concern does not have a Controlling Interest in the entity.

Under penalties of perjury, I declare that I have read the foregoing statement and that the facts stated in it are true.

Printed Name: _____ Title: _____

Signature: _____ Date: _____

[FL DMS PUR 1355](#) 10/23

VENDOR AFFIDAVIT REGARDING THE USE OF COERCION FOR LABOR AND SERVICES

Vendor Name: _____

Address: _____

Section 787.06(13), Florida Statutes requires all nongovernmental entities (such as Vendor) executing, renewing, or extending a contract with a governmental entity (such as the School Board of Levy County, Florida) to provide an affidavit signed by an officer or representative of Vendor under penalty of perjury that Vendor does not use coercion for labor or services as defined in that statute.

As the person authorized to sign on behalf of Vendor, I certify that the company identified above does not:

- Use or threaten to use physical force against any person;
- Restrain, isolate, or confine or threaten to restrain, isolate, or confine any person without lawful authority and against her or his will;
- Use lending or other credit methods to establish a debt by any person when labor or services are pledged as a security for the debt, if the value of the labor or services as reasonably assessed is not applied toward the liquidation of the debt, the length and nature of the labor or services are not respectively limited and defined;
- Destroy, conceal, remove, confiscate, withhold, or possess any actual or purported passport, visa, or other immigration document, or any other actual or purported government identification document, of any person;
- Cause or threaten to cause financial harm to any person;
- Entice or lure any person by fraud or deceit; or
- Provide a controlled substance as outlined in Schedule I or Schedule II of s. 893.03 to any person for the purpose of exploitation of that person.

Under penalties of perjury, I declare that I have read the foregoing document and that the facts stated in it are true.

Printed Name: _____ Title: _____

Phone Number: _____ Email Address: _____



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 the 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 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) 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.



Terms of Use

NOTICE: We have updated our Terms of Use effective May 31, 2023. We did this primarily (1) to notify Users about our COPPA, FERPA, and California Student Privacy certifications issued by iKeepSafe (please see below for more information); (2) to create more consistency in how we explain our student data practices across these Terms, our Privacy Policy, and our Client Agreements; and (3) to add language about new laws that may apply to you. We believe the rights and obligations of Users and Apptegy did not materially change as a result of this update. However, we encourage you to review the updated Terms of Use below, which applies to all Users of the Services on a going-forward basis.

*** **

Last updated: May 31, 2023

Thank you for choosing Apptegy, Inc. (collectively, including our subsidiaries and affiliates, “**Apptegy**,” “**we**,” “**us**,” or “**our**”). These Terms of Use (the “**Terms**”) explain the agreement you make with Apptegy when you access or use any of our websites, software, platforms, mobile applications, and other digital resources and services, including, but not limited to:

- our websites, including www.apptegy.com, www.thrillshare.com, and www.edurooms.com (collectively, the “**Sites**”);
- our Thrillshare platform (“**Thrillshare**”), which collectively includes:
- our Media platform (“**Media**”),
- our Engage platform (“**Engage**”),
- our Rooms platform (“**Rooms**”); and
- any other platforms or tools that we choose to add to Thrillshare; and
- any website and/or mobile application that provides access to and use of any of the foregoing

(collectively, including the Sites, Thrillshare, Media, Engage, Rooms, and all services related to the foregoing, the “**Services**”).

These Terms apply to you and all other Users of the Services. “**Users**” include:

- Clients (as defined below);
- End Users (as defined below); and
- Visitors (as defined below).

For the sake of clarity, references to “**Users**” and “**you**” in these Terms refer to you as a User individually and to all Users collectively, unless expressly set out otherwise.

PLEASE REVIEW THESE TERMS CAREFULLY. We have attempted to provide transparent explanations of our practices and policies so you can make a meaningful decision about whether to use the Services.

BY USING THE SERVICES IN ANY WAY, INCLUDING USING THE SERVICES AS AN END USER OR ONLY AS A VISITOR, YOU AGREE TO BE BOUND BY EVERYTHING IN THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS IN FULL, YOU MAY NOT USE THE SERVICES AND YOU SHOULD STOP USING THE SERVICES IMMEDIATELY.

IMPORTANT NOTE ABOUT INTEGRATION WITH SEPARATE CLIENT AGREEMENTS

Some Users have a direct business relationship with us (individually, a “**Client**” and collectively, “**Clients**”). Our Clients are typically education institutions, government bodies, and other organizations. Clients execute a separate order form and client agreement with us that includes additional terms and conditions for the Services and for our business relationship (a “**Client Agreement**”).

If you are a User and also a Client, the terms and conditions of our Client Agreement are in addition to these Terms; *provided* you are also subject to these Terms as follows:

- the terms and conditions of the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement; and
- the terms and conditions of these Terms will control and govern with respect to all matters not expressly addressed in the Client Agreement.

Not all Users are Clients. Most individuals that access or use the Services are invited or added to the Services by a Client under the Client’s account with us (for example: teachers, students, parents, and guardians invited or added to the Services by their education institution). Some individuals only visit the public parts of the Services that do not require a log-in or an invitation from a Client (for example: individuals browsing the Sites). In these terms we call individual end users using the Services under a Client account “**End Users**” and call individual visitors to the public parts of the Services “**Visitors**.” All individual Users are either End Users or Visitors.

We do not offer or provide Client accounts for individuals, including End Users or Visitors. This means that End Users and Visitors are not Clients and will not have a Client Agreement separate from these Terms. If you are a User without a Client Agreement, including End Users and Visitors, these Terms will control and govern in all circumstances.

1. Summary of the Terms

The Services are communication and group management tools. Apptegy provides the Services for you to use in your sole discretion and at your own risk, except as expressly set out in these Terms. You are exclusively responsible and liable for your use of the Services and for any consequence of your use of the Services to you and to all third parties. Apptegy does not participate in, is not a party to, and is not liable for the activities of Users on or through the Services. More information is available below.

We collect, store, and use personal information in the ways we explain below and in our Privacy Policy. Apptegy respects and values the privacy of personal information, and we work hard to protect it. We have attempted to provide transparent explanations of our privacy practices and policies so you can make a meaningful decision about whether to use the Services.

Apptegy works hard to keep your personal information secure. That said, no technology company can guarantee absolute data security. For more information about our security practices, please continue to read below and review our Privacy Policy.

We rely on third party providers for parts of the Services. The parts of the Services that rely on or implement third party products or services may also be subject to the practices and policies of the applicable third party provider, which may be different than ours. More information is available below and in our Privacy Policy.

By using the Services, you agree that Apptegy will not be responsible or liable to you or any third party for any consequence, loss, or damage arising (directly or indirectly) from or relating to your use of the Services, unless and only as specifically described otherwise in these Terms. More information is available below.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

2. Personal Information and Privacy Generally

By using the Services, you acknowledge and agree that Apptegy collects, stores, and uses certain personal information about Users. To understand what personal information we collect, store, and use, please review our Privacy Policy:

- <https://www.apptegy.com/privacy-policy/>.

The Privacy Policy applies to all Users and for all Services generally. By using the Services in any way, you understand and acknowledge that the terms of our Privacy Policy apply to you in all circumstances. Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

3. Children's Personal Information and Privacy

Apptegy does not intentionally request, collect, store, or use personal information from or about any child under the age of legal majority for our own purposes. Instead, we prohibit use of the Services by children under the age of legal majority, including 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 a Client. When children are invited or added to the Services as Users under Client's account (for example: students attending the educational institution that is the Client), Apptegy provides the Services with respect to the students solely in the educational context authorized by Client under that Client's Client Agreement, and solely for the benefit of the Client and its Users. We only request, collect, store, and use personal information about children as is necessary to provide the Services to our Clients and Users, and only as directed by the Client, as explained more fully below and in our Privacy Policy. If we learn that we have unintentionally collected personal information from or about a child other than as set out below and in our Privacy Policy, we will delete that information as soon as reasonably practicable.

When children are invited or added to the Services as Users under Client's account, Apptegy may receive and collect information from or about children as a necessary part of providing the Services to the 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). These Terms and our Privacy Policy, accessible as set out above, provide notice regarding Apptegy's collection, use, and disclosure of personal information from children. Please see the Privacy Policy for more detailed information, specifically including Section 8 of the Privacy Policy.

Please see our Privacy Policy for information about our Children's Online Privacy and Protection Act ("**COPPA**") and Family Educational Rights and Privacy Act ("**FERPA**") practices and policies.

4. User Eligibility

To use the Services, you must be a Client, an End User invited or added to the Services by a Client, or a Visitor. By using the Services, you represent that you are one of these types of Users. Any use of or attempt to use the Services in any other capacity is void.

When you use the Services, Apptegy grants you a limited, personal, revocable, non-transferable, and non-exclusive license to use the Services subject to these Terms. This limited license is only so you may use the Services as allowed under these Terms, solely for your internal purposes if you are a Client and solely for your personal purposes if you are an End User or Visitor. You may not use the Services for any Prohibited Use or Content (as defined below). This license is revocable at will and may be terminated by Apptegy without notice to you.

Parts of the Services require you to register for, or access and use the Services under, an account. Clients have Client accounts. End Users have End User accounts. Visitors are not permitted to create an account. We request certain account information from or about Clients and End Users to provide the Services. You agree to provide truthful and complete information for and in connection with your account. If you choose to not provide certain account information or fail to complete account information requests, parts of the Services may not be available to you or may not function as intended. We treat personal information you provide in connection with your account in accordance with our Privacy Policy.

Clients may manage their account via the Services or by contacting us. End User accounts are created, controlled, and managed by the Client that invited or added you to the Services (for example: the educational institution that is your employer or that you attend as a student). If you are an End User, your Client account administrator(s) may be able to manage, access, change, edit, disable, or deactivate your account, your account information, or your log-in credentials without our or your involvement or consent. End Users that want to manage, access, change, edit, disable, or deactivate their account, account information, or log-in credentials must contact the Client that invited or added them to the Services (for example: the educational institution that is your employer or that you attend as a student). End Users are also subject to the account practices and policies of the applicable Client. The Client's practices and policies may be materially different than our practices and policies. Apptegy expressly disclaims all liability for the foregoing.

Use of the Services by individuals under the age of legal majority in their jurisdiction of residence is expressly prohibited, unless and only to the extent the individual is an End User invited or added to the Services by a Client (for example: a student using the Services set up by their education institution). If you are an individual User under the age of legal majority in your jurisdiction of residence, a parent or legal guardian must agree to these Terms on your behalf and consent to your use of the Services, and that parent or legal guardian will be exclusively responsible and liable for your use of the Services and for any consequence of your use of the Services. Any attempt by an individual under the age of legal majority in their jurisdiction to use the Services in any capacity without the agreement and consent of a parent or guardian is void. For all End Users under the age of legal majority in their jurisdiction of residence, Apptegy exclusively relies on the Client to obtain the required legal consents from a parent or legal guardian. Please see Section 3 above and our Privacy Policy for more information about use of the Services by Users under the age of legal majority.

If you are using the Services as or on behalf of an individual other than yourself, you represent that you are authorized and have express prior consent to act for and bind that other person to these Terms. If you are using the Services on behalf of an entity, you represent that you are authorized and have express prior consent to act for and bind that entity to these Terms.

Apptegy reserves the right to determine in our sole discretion whether your access or use of the Services fails to satisfy the terms of this Section 4. Failure to comply with the terms set out in this section will be a breach of these Terms and may result in termination of your use of the Services and liability for damages. You agree that Apptegy will not be liable, and you will indemnify, hold harmless, and reimburse Apptegy for any consequence, loss, damage, or expense (direct or indirect) (including attorneys' fees and settlement amounts) arising from or relating to your failure to comply with the terms set out in this section.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

5. Your Obligations as a User; Acceptable Use and Content on the Services

You agree to access and use the Services only in accordance with these Terms and applicable law. You agree to not:

- provide personal or confidential information on or via the Services that you expect to be treated differently than as described in these Terms and our Privacy Policy;
- use the Services in violation of any laws (including data privacy and intellectual property laws) or to promote illegal or tortious activities;
- use the Services in a manner that is false, fraudulent, or deceptive;
- use the Services to threaten, abuse, harass, attack, defame, or harm others, or to post violent, obscene, vulgar, hateful, pornographic, profane, indecent, discriminatory, or otherwise illegal or inflammatory content;
- use the Services for consumer marketing or advertising, commercial solicitations, or for junk mailing or spamming;
- use the Services for political or campaign messaging;
- misuse any reporting, flagging, or complaint tool, including by making submissions without sufficient grounds;
- use the Services to breach, circumvent, disable, disrupt, damage, monitor, tamper, or otherwise interfere with Apptegy, the Services or any part of the Services, any User, or any related equipment, system, network, or security or authentication measure, by any method (including

phishing, overloading, flooding, spamming, spoofing, scraping, or by posting, uploading, sharing, or otherwise providing content that contains viruses, malware, bots, worms, script exploits, or other malicious code);

- use the Services to determine, copy, modify, translate, create derivative works of, design around, benchmark, or reverse engineer the Services or any part of the Services;
- sublicense, sell, assign, or otherwise transfer the Services or any rights under these Terms to a third party, or otherwise commercially exploit or profit from the Services in any manner, except as expressly permitted by these Terms;
- solicit Users to use other services that are competitive with or a replacement for Apptegy;
- falsely imply affiliation with or sponsorship by Apptegy without the prior written consent of Apptegy; or
- breach any of the terms or conditions of these Terms or our Privacy Policy (collectively, **“Prohibited Use or Content”**).

You are solely responsible and liable for all activity that occurs on and through the Services under or in connection with your account. THIS SPECIFICALLY INCLUDES ALL CONTENT AND COMMUNICATIONS POSTED, UPLOADED, SHARED, OR OTHERWISE PROVIDED ON OR VIA THE SERVICES UNDER OR IN CONNECTION WITH YOUR ACCOUNT, AND ANY CONSEQUENCE, LOSS, OR DAMAGE (DIRECT OR INDIRECT) CAUSED BY OR RELATED TO THE FOREGOING.

You must actively monitor the use of the Services under or in association with your account. You are solely responsible and liable for maintaining and safeguarding the security and accuracy of your account, as well as ensuring that all use of the Services by you or in connection with your account does not violate these Terms. You must promptly notify us of any unauthorized access or use.

Apptegy does not, as a general rule, actively monitor the actions of individual Users on or via the Services, but we reserve the right to do so at any time and for any reason. Apptegy expressly disclaims all liability for the foregoing. YOUR ACCESS AND USE OF THE SERVICES IS AT YOUR OWN RISK.

Apptegy is not responsible or liable for the actions or omissions of any User on or via the Services, or any consequence thereof. THIS SPECIFICALLY INCLUDES ALL CONTENT AND COMMUNICATIONS POSTED, UPLOADED, SHARED, OR OTHERWISE PROVIDED ON OR VIA THE SERVICES BY USERS, AND ANY CONSEQUENCE, LOSS, OR DAMAGE (DIRECT OR INDIRECT) CAUSED BY OR RELATED TO THE FOREGOING.

Apptegy reserves the right to determine in our sole discretion whether your access or use of the Services fails to satisfy the terms of this Section 5. Failure to comply with the terms set out in this section will be a breach of these Terms and may result in termination of your use of the Services and liability for damages. You agree that Apptegy will not be liable, and you will indemnify, hold harmless, and reimburse Apptegy for any consequence, loss, damage, or expense (direct or indirect) (including attorneys' fees and settlement amounts) arising from or relating to your failure to comply with the terms set out in this section.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

6. Our Rights as Apptegy

Apptegy exclusively owns and holds all rights, title, and interests in and to the Services and all intellectual property rights arising from or related to the Services. Users do not acquire any such rights by using the Services. The Services are currently (or may be in the future) protected by copyright, trademark, patents, trade secrets, and other laws of both the United States and foreign countries. Other than as expressly provided in these Terms, you do not have any right to use, copy, or imitate the name "Apptegy" or any of the Apptegy trademarks, logos, domain names, distinctive brand features, or other intellectual property or content, in whole or in part, without our prior written permission.

By using the Services, you grant Apptegy a non-exclusive, limited, revocable license during the term to upload, use, copy, store, transmit, and display all information, content, communications, posts, publications, and other material stored or uploaded by you and under or in association with your account (collectively, "**User Content**") to the extent necessary to provide the Services to you. All rights, title, and interests in and to User Content will remain exclusively with the applicable User; *provided* that Apptegy is permitted to aggregate and use generalized and deidentified User Content for any purpose in our sole discretion in accordance with our Privacy Policy.

If you are an End User of the Services under a Client account, you acknowledge that your individual rights with respect to User Content will also be subject to the practices and policies of the applicable Client (for example: the educational institution that is your employer or that you attend as a student). The Client's practices and policies may be materially different than our practices and policies. Apptegy expressly disclaims all liability for the foregoing.

We reserve the right to terminate, suspend, change, or refuse to provide all or any part of the Services, to restrict or limit use of all or any part of the Services, to suspend or terminate any User, and to change eligibility criteria for Users – all at any time and for any reason in our sole discretion, and without notice or liability to you.

Feedback, ideas, and suggestions you provide (“**Feedback**”) about Apptegy or the Services is welcome and is entirely voluntary. You grant Apptegy an exclusive, unlimited, unrestricted, perpetual, irrevocable, worldwide, royalty-free, transferable license to use all Feedback in our sole discretion, including for modifying the Services and for other commercial uses. This license includes all intellectual property rights in and to all Feedback. By providing Feedback, you agree that our right to use Feedback is without restriction and solely in our discretion.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

7. Support Services

We will respond to all questions about or relating to the Services within a reasonable period of time during normal business hours. We will use commercially reasonable efforts to ensure that the Services are accessible 24 hours a day, 7 days a week, and to minimize the amount of time the Services are unavailable. We are not responsible for Users’ internet connections or equipment. You acknowledge and agree that from time to time the Services may be inaccessible or inoperable.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

8. Confidential Information; Disclosure of User Information

You and Apptegy each agree to keep confidential and to not disclose to any third party the non-public confidential and/or proprietary information of the other party, and to only use such information as required in connection with the Services or as expressly permitted by these Terms. Breach of the foregoing obligation will cause irreparable harm for which monetary damages would be inadequate. If a breach occurs or is threatened, the party from which the applicable information originated will be entitled to seek an injunction, a restraining order, or other equitable remedy, in addition to all other available remedies. That party will not need to post a bond or other security or provide proof of actual damages.

Apptegy will seek to protect User information from disclosure in most instances as a general policy. However, we reserve the right in our discretion to access, read, preserve, and disclose User information that we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process, or governmental request; (ii) enforce these Terms, including investigation or prosecution of potential violations or abuse; (iii) detect, prevent, or otherwise address fraud, security, or technical issues; (iv) respond to User support requests; (v) comply with any lawful

requests for information from the Client that has paid for or is otherwise providing your access to the Services; and (vi) protect the rights, property, or safety of Apptegy, our Users, or the public.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

Please see our Privacy Policy for additional information.

9. Termination

These Terms apply to you until your use of the Services is terminated. If you are a Client, you may terminate your use of the Services in accordance with your Client Agreement. If you are an End User, you may terminate your use of the Services at any time in your discretion, however your End User account may be terminated only by the Client that invited or added you to the Services (for example: the educational institution that is your employer or that you attend as a student). If you are a Visitor, you may terminate your use of the Services in your discretion. Apptegy reserves the right to terminate all or any part of the Services and to terminate any User at any time and for any reason in our sole discretion, and without notice or liability to you. Without limiting the generality of the foregoing, examples of when Apptegy may terminate your use of the Services include (i) when you have violated these Terms, the Privacy Policy, a Client Agreement, or other published policies; (ii) when you create risk of or possible legal exposure for Apptegy; or (iii) when the Services are no longer commercially viable.

In all such cases, your license to use the Services will automatically be canceled, except that the following sections will continue to apply: 2, 3, 5, 6, 8, 10, 11, and 12, as well as any other provision that would logically survive termination or expiration.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

10. Disclaimers and Limitations of Liability; Your Risks and Responsibilities

PLEASE READ THIS SECTION CAREFULLY. This section limits the liability of Apptegy and its past, present, and future parents, subsidiaries, affiliates, related companies, officers, directors, employees, agents, representatives, partners, and licensors (collectively, the “**Apptegy Entities**”). **BY USING THE SERVICES, YOU EXPRESSLY AGREE TO BE BOUND BY THIS SECTION.** Each subsection below applies to the maximum extent permitted under applicable law. Some jurisdictions do not allow the disclaimer of certain warranties or the limitation of liability in contracts, and, as a result, the contents of these sections may not apply to you.

Notwithstanding anything to the contrary in this Section 10, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

A. Use is at Your Own Risk; The Services are Available “AS-IS”

Apptegy has no fiduciary or other special relationship with you. YOUR ACCESS TO AND USE OF THE SERVICES IS AT YOUR OWN RISK. You understand and agree that the Services are provided to you on an “AS IS” and “AS AVAILABLE” basis.

To the maximum extent permitted under applicable law, except as expressly set out in these Terms, THE APPTEGY ENTITIES DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, SECURITY, ACCURACY, AND ANY WARRANTIES IMPLIED BY PERFORMANCE OR USE. APPTEGY DOES NOT WARRANT THAT THE SERVICES ARE ERROR-FREE. THE SERVICES MAY ALSO BE UNAVAILABLE, INTERRUPTED, OR DELAYED FOR VARIOUS REASONS (INCLUDING MAINTENANCE AND INTERRUPTIONS INHERENT IN THE AVAILABILITY OF THE INTERNET AND THIRD PARTY MESSAGING SYSTEMS).

Except as is expressly set out in these Terms and the Privacy Policy, the Apptegy Entities make no warranty and disclaim all responsibility and liability for: (i) the completeness, accuracy, availability, timeliness, security, and reliability of the Services; (ii) any harm that results from your access to or use of the Services; (iii) the deletion of, or the failure to store or to transmit, any information and other communications maintained by the Services; (iv) whether the Services meet your requirements or are available on an uninterrupted, secure, or error-free basis; and (v) any third party claims, consequence, loss, or damage (direct or indirect) arising in any way out of or related to use of the Services or these Terms. No advice or information, whether oral or written, obtained from the Apptegy Entities or through the Services, will create any warranty not expressly made in these Terms.

IT IS THE EXCLUSIVE RESPONSIBILITY OF EACH USER TO EVALUATE THE RISK, ACCURACY, COMPLETENESS, DEPENDABILITY, USEFULNESS, AND MARKETABILITY OF THE SERVICES, AND ANY CONTENT OR INFORMATION AVAILABLE THROUGH THE SERVICES OR OBTAINED FROM ANOTHER USER, THIRD PARTY, OR LINKED SITE.

B. Third Party Links and Resources

The Services may contain links to third party products, websites, and resources. Except as expressly set out in the Services, you agree that the Apptegy Entities are not responsible or liable for: (i) the availability or accuracy of third party products, websites, or resources; (ii) the content, products, or services on or available from third party websites or resources; and (iii) any

consequence, loss or damage (direct or indirect) arising from third party products, websites, or resources. Inclusion of third party products, websites, or resources does not imply endorsement by the Apptegy Entities of the websites, resources, or the content, products, or services available from the third parties. You acknowledge sole responsibility for and assume all risk of your use of any third party product, website, or resource.

C. Third Party Providers and Partners

Apptegy relies on third party providers and partners for parts of the Services (for example: posting a communication on a Facebook or Twitter account; or language translations). Apptegy may also engage third parties to perform certain Services. Except as expressly set out on in these Terms or the Privacy Policy, you agree that the Apptegy Entities are not responsible or liable for: (i) the availability, functionality, or accuracy of the parts of the Services provided by third party providers and partners; (ii) any interruption, delay, suspension, or termination of the Services as a result of third party providers and partners; and (iii) any consequence, loss, or damage (direct or indirect) arising from or relating to third party providers and partners. On written request by a User, Apptegy will provide within a reasonable time a list of the non-confidential third party providers and partners that Apptegy uses for the Services at that time.

If you register for or log on to the Services by using existing third party accounts or profiles (for example: login via Google, Facebook, Twitter, etc.) and/or use third party services accessible via the Services (for example: posting a communication on a Facebook or Twitter account), you agree that you will also be subject to the third party practices and policies associated with the third party services that you use. The practices and policies of the applicable third parties may be materially different than our practices and policies, including with respect to data privacy and security. YOUR ACCESS AND USE OF THIRD PARTY SERVICES IS AT YOUR OWN RISK.

Without limiting the generality of the foregoing, YOU AGREE THAT 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, AND/OR YOUR USE OF THE SAME.

Please see our Privacy Policy for more information.

D. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE APPTEGY ENTITIES WILL NOT BE RESPONSIBLE OR LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUE, USE, GOODWILL, OR OTHER INTANGIBLE LOSSES, WHETHER INCURRED DIRECTLY OR

INDIRECTLY BY YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE APPTTEGY ENTITIES WILL NOT BE RESPONSIBLE OR LIABLE FOR ANY HARM, DAMAGES, OR LOSS ARISING FROM OR RELATING TO (i) YOUR ACCESS TO OR USE OF (OR INABILITY TO ACCESS OR USE) THE SERVICES; (ii) ANY CONDUCT OR CONTENT OF ANY USER OR THIRD PARTY ON OR THROUGH THE SERVICES, INCLUDING WITHOUT LIMITATION, PERSONAL INJURY, PROPERTY DAMAGE, AND DEFAMATORY, OFFENSIVE, OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES; (iii) ANY INFORMATION OR CONTENT VIEWED OR OBTAINED FROM THE SERVICES; OR (iv) UNAUTHORIZED ACCESS, USE, OR ALTERATION OF THE SERVICES. IN NO EVENT WILL THE AGGREGATE LIABILITY OF THE APPTTEGY ENTITIES EXCEED THE GREATER OF ONE THOUSAND U.S. DOLLARS (U.S. \$1,000.00) OR THE AMOUNT PAID TO APPTTEGY BY YOU FOR THE SERVICES IN THE PRIOR TWELVE (12) MONTHS. FOR FREE USES OR TRIAL USES, APPTTEGY'S TOTAL LIABILITY WILL NOT EXCEED ONE HUNDRED U.S. DOLLARS (U.S. \$100.00). THE FOREGOING REMEDY WILL CONSTITUTE THE APPTTEGY ENTITIES' SOLE LIABILITY AND OBLIGATION WITH RESPECT TO ANY CLAIM BY YOU.

THE LIMITATIONS OF THIS SUBSECTION WILL APPLY TO ALL THEORIES OF LIABILITY, WHETHER BASED ON PERSONAL INJURY, PROPERTY DAMAGE, WARRANTY, CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, WHETHER OR NOT THE APPTTEGY ENTITIES HAVE BEEN INFORMED OF THE POSSIBILITY OF ANY SUCH DAMAGE, AND EVEN IF A REMEDY SET OUT IN THIS AGREEMENT IS FOUND TO HAVE FAILED ITS ESSENTIAL PURPOSE.

IF YOU ARE A CALIFORNIA RESIDENT, YOU HEREBY WAIVE YOUR RIGHTS UNDER CALIFORNIA CIVIL CODE 1542, WHICH STATES "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR."

E. Monitoring the Services

As set out in these Terms, Clients and End Users (for example: teachers, students, parents, and guardians using the Services set up by their education institution) are solely responsible for all User information, content, and messages that are communicated or published via the Services (for example: communications published by an educational institution via Media, or communications and materials posted by a student or teacher via Rooms). It is possible that some User content may be inappropriate and/or constitute Prohibited Use or Content. You are solely responsible and liable for monitoring the Services to ensure that User content is not inappropriate. If you are an End User and discover inappropriate User content, you should promptly notify the Client that invited or added you to the Services (for example: the educational institution that is your employer or that you attend as a student). If you are a Client and discover or are made aware of inappropriate User content on

or under your Client account, you should remove it promptly. If you are unable to remove it, please contact us and we will use commercially reasonable efforts to assist you. Apptegy does not, as a general rule, actively monitor the actions of individual Users on or via the Services, but we reserve the right to do so at any time and for any reason.

Parts of the Services include features that allow Users to flag User content as inappropriate. When a User flags User content as inappropriate, the Client that is associated with the flagged User content receives notice (for example: the educational institution that is the Client). In all such events, the Client is exclusively responsible and liable for reviewing the flagged content, and exclusively responsible and liable for determining whether to remove or permit the flagged content, and whether any other action is necessary or appropriate. Please note that the content flagging feature may be disabled and will only be available to End Users if the Client that invited or added you to the Services (for example: the educational institution that is your employer or that you attend as a student) chooses to enable it.

Apptegy disclaims all responsibility and liability for the availability, completeness, timeliness, reliability, accuracy, and decision-making with respect to monitoring User actions and User content on the Services, and the review or non-review of flagged User content, as well as all harm, claims, consequences, losses, and damages (direct or indirect) arising in any way out of or related to all User content, flagged User content and the review or non-review thereof, and any action or non-action related to any of the foregoing. The Apptegy Entities will not be liable in any manner or form, or under any theory or cause of action, for inappropriate content or materials posted on or communicated via the Services, or any review or lack thereof of such content or materials, or any action or non-action related to any of the foregoing, unless Apptegy is the author of the content or materials. No advice or information, whether oral or written, obtained from the Apptegy Entities or through the Services will create any liability or obligation for Apptegy with respect to User content that is not expressly made in these Terms.

PLEASE NOTE that if you discover or are made aware of any User content that is or may be connected to the abduction or sexual exploitation of a child, you should contact law enforcement authorities immediately. Please see the National Center for Missing and Exploited Children (NCMEC) (www.missingkids.org/education) for more information and resources related to abduction and child sexual exploitation prevention.

F. Alerts

If you purchase and/or use the alerts feature of the Services, you acknowledge and agree that we provide alerts functionality only as a non-emergency communication tool. You acknowledge and agree that the Services are not intended to be and cannot be used as a substitute for emergency communication methods (for example: contacting law enforcement and/or emergency medical professionals in the event of a threat to person or property; or providing notice of an emergency).

Traditional emergency communications should be completed before using the Services in any such event. Clients and End Users, as applicable, are solely responsible and liable for use of the alerts feature and the completeness, timeliness, reliability, accuracy, omission, and decision-making with respect to all alerts content. You are solely responsible and liable for your own reliance on alerts or lack thereof, and all alert content.

Apptegy disclaims all responsibility and liability for the completeness, timeliness, reliability, content, accuracy, omission, and decision-making with respect to all alerts or lack thereof, and all harm, claims, consequences, losses, and damages (direct or indirect) arising in any way out of or related to all alerts or lack thereof. Apptegy Entities will not be liable in any manner or form, or under any theory or cause of action, for alerts or lack thereof, or alert content, posted on or communicated via the Services unless we post the content or materials. No advice or information, whether oral or written, obtained from the Apptegy Entities or through the Services will create any liability or obligation for Apptegy with respect to alerts or alert content that is not expressly made in these Terms.

G. Translations

When using the Services, you may see or receive content that has been translated from English to another language, or vice versa. In those circumstances, the Services have been translated for your convenience only and may have been translated using third party translation software. Reasonable efforts have been made to provide an accurate translation; *however*, no translation is perfect, nor is automated translation intended to replace human translators. Translations are provided to you solely on an “AS IS” and “AS AVAILABLE” basis. No warranty of any kind, either express or implied, is made as to the accuracy, reliability, or correctness of any language translation. Some content (for example: images, videos, Flash, etc.) may not be accurately translated due to the limitations of translation software.

The official text is the English version of the Services. Any discrepancies or differences created in translation are not binding and have no legal effect for compliance or enforcement purposes. If you have a question related to the information contained in translated Services, please refer to the official English version of the Services.

Without limiting the generality of the foregoing, the Services may contain translations powered by Google Translate. Google disclaims all warranties related to the translations, express or implied, including any warranties of accuracy, reliability, and any implied warranties of merchantability, fitness for a particular purpose and noninfringement.

H. Electronic Signatures

Parts of the Services include features that allow Users to electronically sign documents and forms. You agree that (i) the Client that invited or added you to the Services (for example: the educational institution that is your employer or that you attend as a student) and its End Users exclusively control and have sole responsibility for all documents, forms, agreements, information, content, communications, and other material submitted to you for electronic signature (collectively, “**Esign Content**”); and (ii) you exclusively control and have sole responsibility for evaluating the accuracy, completeness, and appropriateness of all Esign Content and for choosing whether to electronically sign any Esign Content. Please note that (i) certain types of forms, documents, agreements, and other materials may be excluded, limited, or otherwise restricted by electronic signature laws and regulations, and/or (ii) certain laws and regulations may impose specific requirements, limitations, and restrictions on specific types of electronic signature content and requests. Clients and End Users, as applicable, are solely responsible and liable for complying with all such laws and regulations. Apptegy disclaims all responsibility and liability for all electronic signature content and requests, and all harm, claims, consequences, losses, and damages (direct or indirect) arising in any way out of or related to all electronic signature content and requests. Apptegy Entities will not be liable in any manner or form, or under any theory or cause of action, for electronic signature content and requests, posted on or communicated via the Services unless Apptegy is the author of the content or request.

I. Accessibility Compliance

Clients are solely responsible for complying with all applicable laws and regulations governing accessibility of the parts of the Services under the control of the Client (for example: a Client’s website and/or mobile applications, and Client and End User activities on the Services, including communications), 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**”). We encourage Clients 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 Clients with accessibility compliance, and Apptegy may provide Clients with materials and information about such laws and regulations, including the ADA and the WCAG. All such tools, materials, and information are provided to assist Clients with their compliance obligations and for general education purposes only. Apptegy disclaims all responsibility and liability for compliance with all laws and regulations governing accessibility of the parts of the Services under the control of Clients (for example: a Client’s website and/or mobile applications, and Client and End User activities on the Services, including communications), including the ADA and/or the WCAG, and all harm, claims, consequences, losses, and damages (direct or indirect) arising in any way out of or related to accessibility, or lack thereof, to the parts of the Services under the control of Clients. Apptegy Entities will not be liable in any manner or form, or under any theory or cause of action, for compliance with any laws and regulations governing accessibility of the parts of the Services under the control of Clients.

J. How These Terms Apply Across Different Services

These Terms apply to all parts of the Services, unless and only to the extent expressly set out in these Terms. Any exceptions will be clearly explained in these Terms. For example, if a specific term or condition does not apply, or applies differently, to Media as compared to Rooms, or to one feature of Media as compared to another feature of Media, then that difference will be explained in these Terms. If you do not see a specific difference or exception listed in these Terms, then it is not a difference or exception, and the general term or condition applies to all parts of the Services.

11. Indemnification

By using the Services, to the maximum extent permitted by applicable law, you agree to indemnify, hold harmless, and reimburse the Apptegy Entities (as defined above) for all claims and liabilities (actual and threatened), obligations, settlements, losses, expenses, debts, and damages (including costs and attorneys' fees) (collectively, "**Claims**") that arise from or relate to (i) your breach of any part of these Terms or our Privacy Policy, including any activity and content associated with your account (whether by you or a third party), (ii) information or materials you post, upload, share, or otherwise provide on or through the Services; (iii) your infringement or violation of copyright, patent, trademark, trade secret, or other intellectual property or related rights of any third party; (iv) any third party services that you access or use via the Services; and/or (v) your negligent or willful misconduct; unless a court of competent jurisdiction enters a final judgment that the Claim was the result of affirmative and intentional actions or omissions by Apptegy. You agree to promptly notify Apptegy of any actual or potential Claim of which you become aware. Apptegy reserves the right to assume exclusive control of and direct the defense or settlement of any third party Claim otherwise subject to indemnification by you. You agree to assist and cooperate with Apptegy in the defense upon request.

Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

12. Miscellaneous

Notwithstanding anything to the contrary in this Section 12, for Users with a Client Agreement, the Client Agreement will control and govern with respect to all matters expressly addressed in the Client Agreement, and those terms and conditions may differ from those set out in this section.

A. Waiver and Severability

The failure of Apptegy to enforce any right or term of these Terms will not be a waiver of the right or term. If any term is held to be invalid or unenforceable, then that term will be limited or eliminated

to the minimum extent necessary, and the remaining parts of these Terms will stay in full force and effect. In such an instance, the parties agree that the intent of the original language should be enforceable against the parties to the maximum extent permitted by law.

B. Controlling Law and Jurisdiction

These Terms and any dispute related to the Terms will be governed by the laws of Delaware without regard to conflicts of law principles. Subject to the dispute resolution terms set out in Section 12.C below, all claims and legal proceedings arising in connection with the Services will be brought exclusively in the federal or state courts located in Little Rock, Arkansas, United States, and you consent to the exclusive jurisdiction and venue of those courts.

C. Dispute Resolution

You agree that you will notify Apptegy in writing of any dispute related to the Services. Apptegy will have thirty (30) days from receipt of your written notice to address the dispute before you may initiate any third party action to resolve the dispute. Notice under this section must be addressed to Apptegy, Inc., c/o Notice of Dispute, 2201 Brookwood Drive, Suite 115, Little Rock, Arkansas 72202.

Any dispute arising from or relating to the subject matter of these Terms that is not voluntarily resolved by the parties pursuant to the previous paragraph must be finally settled by arbitration in Little Rock, Arkansas, by JAMS, Inc. (“**JAMS**”) or its successor, under the then applicable JAMS Comprehensive Arbitration Rules & Procedures. Judgment on or enforcement of the arbitration award may be entered in any court having jurisdiction. Any arbitration under this Agreement will take place on an individual basis: CLASS ARBITRATIONS AND CLASS ACTIONS ARE NOT PERMITTED. BY USING THE SERVICES, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE WAIVING THE RIGHT TO TRIAL BY JURY AND TO PARTICIPATE IN A CLASS ACTION.

Notwithstanding the previous obligations, each party will have the right to start an action at any time for injunctive or equitable relief in the mandatory jurisdiction and venue established above. If you are a resident of a jurisdiction where binding arbitration and class action waivers are not valid, this section will not apply to you.

D. Consent to Electronic Communication

By using the Services, you agree to receive all communications related to your use of the Services in electronic form, including, but not limited to, emails sent to the email address associated with your account, and/or posted notices on the Services. By using the Services, you agree that all agreements, notices, disclosures, and other communications from Apptegy that are provided electronically will satisfy all legal requirements that communications be in writing. All notices from

Apptegy will be deemed effective when sent to the email address associated with your account, or when posted publicly on the Services.

E. Entire Agreement; Relationship to Other Agreements; Assignment

These Terms and the Privacy Policy are the entire and exclusive agreement between Apptegy and you about the Services and supersede and replace any prior agreement or understanding between us. Notwithstanding the foregoing, for Users with a Client Agreement, the Client Agreement will also be part of our agreement.

Apptegy may offer additional services to supplement the Services (for example: marketing services). Supplemental services may require you to enter into a separate agreement with us and/or be subject to additional terms specific to the supplemental services. Supplemental services are in the sole discretion of Apptegy.

The agreement established by these Terms is made for the sole benefit of Apptegy and the User, and their respective successors and permitted assigns. Except as expressly provided in these Terms, no other person or entity is intended to or will have the rights or benefits provided under these Terms, whether as third party beneficiaries or otherwise. None of the Terms, nor any right, obligation, or remedy under the Terms is assignable, transferable, or sublicensable by you except with our prior written consent. Any attempted assignment, transfer, or sublicense by you without our prior written consent is null and void. Apptegy may assign, transfer, or delegate these Terms or any right or obligation or remedy under these Terms in its sole discretion.

F. Changes to Terms; Supplemental Terms

We may change these Terms from time to time in our discretion. The most current version will always be at the following link: <https://www.apptegy.com/terms-and-conditions/>. We encourage you to review it regularly. Any changes will be effective immediately upon us posting the updated Terms. If we make updates or changes, we will give notice by updating the posted date for these Terms. In some cases and in our sole discretion, we may provide additional notice (for example: by a pop-up or banner notice on the Services, or by sending you an email notification). By continuing to use the Services after changes are effective, you will be bound by the revised Terms. If you do not agree with any updates to these Terms, you may not continue to use the Services.

Notwithstanding the foregoing, if we make updates or changes that materially change User rights with respect to personal information, or reduce the level of protection for personal information, we will comply with applicable law. We will provide you with advance notice on the Services and, if required by applicable law, request your consent. For impacted Clients, we will also provide notice to you via the contact information you have provided to us. Please return to this page periodically to ensure you are familiar with the most current version of these Terms.

G. Notices; Contact

General Notice. The Services are operated and provided by Apptegy, Inc., 2201 Brookwood Drive, Suite 115, Little Rock, Arkansas 72202. If you have any questions about the Services or these Terms, please contact us at legal@apptegy.com, or by writing to our mailing address, c/o Legal Department.

Notice for California Users. Under California Civil Code Section 1789.3, California users of the Services are entitled to the following specific consumer rights notice: These Services are operated and provided by Apptegy, Inc., 2201 Brookwood Drive, Suite 115, Little Rock, Arkansas 72202. If you have any questions about the Services or these Terms, please contact us at legal@apptegy.com or by writing to our mailing address, c/o Legal Department. California residents may reach the Consumer Assistance Unit of the Consumer Information Division of the California Department of Consumer Affairs, which may be contacted in writing at 1625 N. Market Blvd., Suite N 112, Sacramento, California 95834, or by telephone at (800) 952-5210 or hearing-impaired persons may dial 711, 1-800-735-2929 (TTY), or 1-800-735-2922 (Voice) for California Relay Service.

Please feel free to contact us with respect to any question about the Services or these Terms at:

- 1-888-501-0024
- legal@apptegy.com
- Apptegy, Inc., 2201 Brookwood Drive, Suite 115, Little Rock, Arkansas 72202

By accessing or using the Services in any manner, including using the Services as an End User or only as a Visitor, you agree to and will be bound by all of the terms and conditions contained in these Terms, and all additional terms, conditions, rules, policies, and/or procedures that may be published by Apptegy from time to time on or through the Services, each of which is incorporated by reference and may be updated by Apptegy at any time without notice to you. These Terms apply to all users of the Services without exception.

Effective: May 31, 2023

Privacy Policy

NOTICE: We have updated our Privacy Policy effective May 31, 2023. We did this primarily (1) to notify Users about our COPPA, FERPA, and California Student Privacy certifications issued by iKeepSafe (please see below for more information); (2) to create more consistency in how we explain our student data practices across this Privacy Policy, our Terms of Use, and our Client Agreements; and (3) to add language about new laws that may apply to you. We believe the rights and obligations of Users and Apptegy did not materially change as a result of this update. However, we encourage you to review the updated Privacy Policy below, which applies to all Users of the Services on a going-forward basis.

*** **

Last updated: May 31, 2023

Thank you for choosing Apptegy, Inc. (collectively, including our subsidiaries and other affiliates, “**Apptegy**,” “**we**,” “**us**,” or “**our**”). The privacy and security of personal information is very important to us. We want you to understand what personal information we collect about you, how we collect that information, how we use it, and what your rights are with respect to what we do. This Privacy Policy (“**Policy**”) explains those things.

The key points are:

- “**Personal information**” means any information about an identifiable individual, or any information that may be used to identify an individual when combined with other readily available information. Examples include your name, your email address, or your IP address;
- The personal information we collect about you, how we collect it, and how we use it depends on your relationship with us;
- We collect and use personal information only to provide and improve our Services (as defined below);
- We do not sell or attempt to monetize your personal information with third parties; and
- You have rights and choices that govern how we will handle personal information about you.

The list of key points above is only a summary. Please review the full Policy to find additional information and to better understand our practices, policies, and obligations, and your rights related to the same.

PLEASE REVIEW THIS POLICY CAREFULLY. We have attempted to provide transparent explanations of our practices and policies so you can make a meaningful decision about whether to use the Services.

BY USING THE SERVICES IN ANY WAY, INCLUDING USING THE SERVICES AS AN END USER OR ONLY AS A VISITOR, YOU AGREE TO BE BOUND BY EVERYTHING IN THIS POLICY. Please note that using our Services is your choice. If you do not consent to the collection, use, or disclosure of personal information as described in this Policy, you should not use our Services.

We may change this Policy from time to time in our discretion. Please see Section 12 below for more information.

If you have questions about this Policy, please contact us at any of the following:

- By email at privacy@apptegy.com;
- By telephone at 1-888-501-0024; or
- By mail at Apptegy Inc., c/o Data Protection Officer, 2201 Brookwood Drive, Suite 115, Little Rock, AR 72202.

1. WHO AND WHAT DOES THIS POLICY APPLY TO

This Policy applies to you and all other Users of the Services. “**Users**” include:

- users that have a direct business relationship with us (“**Clients**”);
- individual users that are invited or added to the Services by a Client under the Client’s account with us (for example: teachers, students, parents, and guardians invited or added to the Services by their education institution) (“**End Users**”); and
- individuals that only visit the public parts of the Services that do not require a log-in or an invitation from a Client (for example: individuals browsing the Sites) (“**Visitors**”).

For the sake of clarity, references to “**Users**” and “**you**” in these Terms refer to you as a User individually and to all Users collectively, unless expressly set out otherwise. Please note that End Users may access and use the Services through the separate website and/or mobile application of a Client, and this Policy applies whether you use the Services directly via our products or via a Client website or application. In this Policy we call education institutions and organizations “**Schools.**”

This Policy applies to all of our products and services, including new or additional products and services that we may develop or offer in the future. This includes but is not limited to:

- our websites, including www.apptegy.com, www.thrillshare.com, and www.edurooms.com (collectively, the “**Sites**”);
- our Thrillshare platform (“**Thrillshare**”), which collectively includes:
- our Media platform (“**Media**”),
- our Engage platform (“**Engage**”),
- our Rooms platform (“**Rooms**”); and
- any other platforms or tools that we choose to add to Thrillshare; and
- any website and/or mobile application that provides access to and use of any of the foregoing

(collectively, including the Sites, Thrillshare, Media, Engage, Rooms, and all services related to the foregoing, the “**Services**”).

If you are a California resident, see the California Privacy Notice for California consumers in Section 5.

If you are a European Union or United Kingdom resident, see the EU and UK Privacy notice in Section 6.

If you are a Canadian resident, see the Canadian Residents notice in Section 7.

This Policy applies in conjunction with the Terms of Use (“**Terms of Use**”) for the Services, accessible at <https://www.apptegy.com/terms-and-conditions>. The Terms of Use applies to all Users and for all Services generally, except as expressly set out in the Terms of Use.

2. WHAT We Collect and How We Collect It

What information we collect about you and how we collect it depends on our relationship with you. Specifically:

- If you are a Client (for example: a School that is our Client), then an explanation of what information we collect about you and your End Users, and how we collect it, can be found below in the section 2.A titled “Personal Information from Schools and Under School Accounts”; or
- If you are an End User (for example: a teacher, staff, student, parent, or guardian added to the Services by a School), then information we collect about you is provided either (1) by the School that added you to the Services and manages your use of the Services, (2) by you when you use the Services, or (3) by another End User using the Services under the account of your School. An explanation of what information we collect about you and how we collect it can be

found below in the section 2.A titled “Personal Information from Schools and Under School Accounts”; or

- If you are a Visitor (for example: an individual browsing a public part of the Sites that does not require a log-in or an invitation from a Client) and you do not use the Services as an End User, then an explanation of what information we collect about you and how we collect it can be found below in the section 2.B titled “Visitor Personal information.”

Please note that our Clients are Schools and other government entities. We do not currently offer or provide Client accounts to individuals, including End Users or Visitors. This means that Apptegy does not have direct relationships with individual end users of the Services. However, the Services allow Clients to create individual user accounts for the End Users that the Client wants to authorize under its Client account (for example: teachers, staff, students, parents, and guardians associated with the School). All End User accounts are controlled and managed by the Client that creates them. In this Policy we call the individual End User accounts created by Schools “**School-Created User Accounts**.” We collect limited personal information from or about individuals outside of School-Created User Accounts. This means that nearly all personal information we collect and use is provided either (1) by Schools adding or managing their End Users on the Services, or (2) by End Users using the Services under School-Created User Accounts. Please continue reading below for more information.

2.A Personal Information from Schools and Under School Accounts

As stated above, nearly all of the personal information that we collect is provided to us either by a School on behalf of the End Users associated with the School, or by End Users using our Services under School-Created User Accounts.

A few examples of when this may happen include:

- a School creates School-Created User Accounts for teachers, staff, parents, guardians, and students under the School’s Client account, and includes personal information in the School-Created User Accounts;
- a School administrator, under her or his School-Created User Account, uses the Services to update School-Created User Accounts, and includes personal information in her or his updates;
- a School principal, under her or his School-Created User Account, uses the Services to publish a communication via Thrillshare Media that includes personal information;
- a School teacher, under her or his School-Created User Account, uses the Services to send classroom communications via Thrillshare Rooms that includes personal information;
- a School student, under her or his School-Created User Account, uses the Services to upload and submit classroom content and assignments via Thrillshare Rooms that includes personal

information;

- a parent or guardian of a School student, under her or his School-Created User Account, uses the Services to communicate with a teacher via Thrillshare Rooms, and includes personal information in her or his communications; or
- a School staff member interacts with Apptegy team members to request technical support for the School's Client account, and includes personal information in her or his communications.

In all of these instances, (i) the School determines and controls what personal information it provides to us for its School-Created User Accounts, (ii) the School determines and controls what personal information can be provided to us by End Users using the Services under the School-Created User Accounts; and (iii) the School determines and controls how personal information is and can be used once it is collected from the School and End Users under the School's Client account. In other words, the School determines and controls the purpose, scope, and means for all personal information collected under or in connection with the School's account. This means the School is the data controller of the personal information collected by us in connection with the School's account and the School-Created User Accounts associated with the School.

Because of that, if you are an End User, your School is the party that is primarily responsible for the personal information we collect about you. And your School is the party responsible for determining the purpose, scope, and means of the personal information we collect about you, and whether and how it is used via our Services. We use that information only on behalf of and under the direct control of the School, and not for our own purposes.

We implement safeguards to protect against the loss, disclosure, alteration, or misuse of personal information that is in our care or custody. We protect all personal information in our care or custody with at least the degree of care that would be exercised by a prudent person given the sensitivity of the personal information. Please continue reading below for more information about our security practices.

In all of these circumstances, Apptegy is only a data processor. This means we only carry out and process, via our Services, the activities of and instructions of your School (and End Users using the Services under School-Created User Accounts).

Simply put: when we process activities and instructions from a School that include personal information about you (or by you or another School-Created User Account under a School account), we are not responsible for the disclosures made or the use of your personal information by the School (or School-Created User Account under the School account). It is your School that has the responsibility to protect your privacy in these instances.

Please note that the privacy and security policies of your School may differ from our policies. In those cases, our policies will not overrule or change the separate policies of your School, and our policies will not impact or change your School's separate agreements with and obligations to you. **Instead, the privacy and security policies of your School govern your personal information and your rights with respect to your School, and not our policies.** As such, you are required to work with your School directly with respect to your personal information. For example, if you request a copy of the personal information we hold about you in order to provide the Services, we will direct you to your School for that information.

Even though we are not primarily responsible for your personal information in these circumstances, we still want you to understand what personal information we might collect about you as the data processor providing the Services and how we collect it.

Schools (and End Users under School-Created User Accounts) typically use our Services to publish, upload, manage, store, and/or send communications, messages, announcements, videos, assignments, materials, electronic signature requests, and other content, documents, and information. Thrillshare Media is typically used when the activity is relevant to the School and its End Users generally; Thrillshare Rooms is typically used when the activity is relevant to a particular subset of the School's End Users – usually a classroom or group at the School.

However, personal information may be collected for or as a result of any of the activities permitted on the Services. As explained above, Schools (and End Users under School-Created User Accounts) make these choices and are responsible for them.

Specifically, the following personal information may be collected in connection with the Services:

- Personal information provided by Schools. We collect personal information that Schools use to create and manage School-Created User Accounts. We also collect personal information that Schools include in the communications, messages, announcements, videos, assignments, materials, electronic signature requests, and other content, documents, and information published, uploaded, managed, stored, and/or sent via the Services. Some of this information may contain personal information; and some personal information may be about you. For example: personal information included in announcements made via Media, or personal information included in messages in Rooms. As noted above, however, we only collect this information when provided by Schools and End Users using the Services under School-Created User Accounts (for example: teachers and staff). Personal information provided by Schools may include:
 - Name
 - Phone number

- Email address
 - Gender
 - Age/birthday
 - School year/classification
 - Race/ethnicity
 - Disability
 - Language
 - Attendance information
 - Classes, groups, and subjects taught or participated in
 - Activities/clubs participated in
 - Information recorded in assignments
 - Information recorded in consents and data collection forms
 - Grading and assessment information
 - Achievements/awards
 - Dietary requirements
 - Transportation preferences
 - Communication preferences
 - Parent(s) and guardians(s) for which a student User is associated
 - Student(s) for which a parent or guardian is associated
 - Other information a School uploads
- *Personal information provided by End Users.* We collect personal information that End Users under School-Created User Accounts include in the communications, messages, announcements, videos, assignments, materials, electronic signature requests, and other content, documents, and information published, uploaded, managed, stored, and/or sent via the Services. Some of this information may contain personal information; and some personal information may be about you. For example: personal information included in announcements made via Media, or personal information included in messages in Rooms. As noted above, however, we only collect this information when provided by Schools and End Users using the Services under School-Created User Accounts (for example: teachers and staff). Personal information provided by End Users may include:
 - Name
 - Phone number

- Email address
 - Gender
 - Age/birthday
 - School year/classification
 - Race/ethnicity
 - Disability
 - Language
 - Attendance information
 - Classes, groups, and subjects taught or participated in
 - Activities/clubs participated in
 - Information recorded in assignments
 - Information recorded in consents and data collection forms
 - Grading and assessment information
 - Achievements/awards
 - Dietary requirements
 - Transportation preferences
 - Communication preferences
 - Parent(s) and guardians(s) for which a student User is associated
 - Student(s) for which a parent or guardian is associated
 - Other information an End User uploads
- *Personal information from use of the Services.* We automatically collect information about how the Services are used by End Users under School-Created User Accounts (for example: teachers, staff, students, parents, and guardians). We may also collect information connected with support and technical help for the Services. Some of this information may contain personal information; and some personal information may be about you. Personal information from use of the Services may include:
 - IP addresses used to access the Services
 - Web browsers and operating systems used to access the Services
 - Makes, models, and device IDs used to access the Services
 - General geographic location (but not precise geolocation) of access to the Services
 - Time zone and language of access to the Services

- Pages on the Services that are viewed
 - Features and functions of the Services that are used and how they are used
 - Information provided during or in connection with a customer support request
 - Other information about how Users interact with the Services
- *Personal information provided for accounts.* We collect information that Schools and End Users provide for the creation, administration, and management of Client accounts and School-Created User Accounts. Some of this information is voluntary. However, please note that certain information is required to use and enjoy the Services. Some of this information may contain personal information; and some personal information may be about you. Personal information provided for accounts may include:
 - Contact details
 - User ID
 - School ID
 - Profile information
 - Contact address
 - Contact phone number
 - Email address
 - Log-in Information
 - Password
 - Billing/Payment Information
 - Communication preferences
 - Employment position (for School employee and contractor Users)
 - Other information a School or User uploads
 - Other information necessary or helpful to provide the Services to the Client
 - *Personal information from third parties.* We collect certain information from third parties to measure and improve our Services, and to improve the experience of our Clients and Users. For example, we collect information about how our marketing and promotional campaigns have performed (see Section 4 for more information about marketing and advertising activities). Some of this information may contain personal information; and some personal information may be about you. Personal information from third parties may include:
 - Analytics and usage data
 - IP addresses

- Pages on the Services that are viewed

As explained above, the personal information we collect from Schools and End Users is under the direct control of the School, and we only collect personal information that is reasonably necessary to provide the Services requested by the Client and its End Users. This means that, with respect to any specific Client and its End Users, the types and scope of personal information actually collected by us will depend on the Services being used by the Client and its End Users. Not all categories will be collected or received for every individual.

Except as set out in these policies, we do not collect or scrape additional personal information from the computers, contacts, email accounts, or other personal sources of Users.

Please note that while we have attempted to provide full and fair notice of the personal information that may be collected in connection with our Services, the list above is not exhaustive. We may in some instances collect personal information other than what is set out in the table above. In those circumstances, we will ensure we have appropriate authority or consent for that collection.

If you are an End User and have questions or requests about personal information or rights under your School's Client account or your School-Created User Account, please address your questions and requests directly to your School. If you contact us regarding these questions and requests, we will direct them to your School. If you are a Client and have questions or requests about personal information or rights under your Client account, please contact us by any of the methods set out above in the introduction to these policies or below in the section 10 titled "Contact Us."

2.B Visitor Personal Information; Generalized and Anonymous Information about All Users

If you are a Visitor (for example: an individual browsing a public part of the Sites that does not require a log-in or an invitation from a Client), we collect limited personal information from and about you. We automatically collect information about how the public parts of the Services are used by Visitors. For example, we collect information about the individual pages that are viewed, the features and functions that are used and how they are used, and other information about how Visitors interact with the Services. We also collect information about what web browsers, devices, and IP addresses are used to access the Services, and the general geolocation of that access (but not precise geolocation). Some of this information may contain personal information (for example: IP addresses). Please also note that if you choose to contact us (for example: send us a message via the email or chat function on the Sites), we collect the personal information that you give us (for example: name, phone number, email address, IP address, and anything you include in the body of your message). In these circumstances, you control what information you provide us. If you choose to not provide certain information, parts of the Services may not be available to you or may not function as intended (for example: you may be required to provide certain personal information to send a communication to us). If you have questions or requests about your personal information or

rights as a Visitor, please contact us by any of the methods set out above in the introduction to these policies or below in the section 10 titled “Contact Us.”

We may collect and use generalized, anonymous information about all Users. This information cannot be used to identify you or isolate your personal information. If you have questions or requests about your personal information or rights in connection with our collection of generalized, anonymous information, please contact us by any of the methods set out above in the introduction to these policies or below in the section 10 titled “Contact Us.”

3. How We Use and Disclose Your Information

We use and disclose personal information solely for the purpose of providing and improving our Services to and for our Clients and Users. We do not sell or otherwise monetize personal information by selling or sharing it with third parties. Specifically, we use and disclose personal information in the following ways:

- *To provide and operate our Services:* We may use and disclose personal information when we are directed or instructed to do so by a Client or an End User under a School-Created User Account. A few examples of when this may happen include: when a School uploads information to setup its Client account, or when a School creates, maintains, and updates School-Created User Accounts, or when an End User posts a communication on the Services that includes personal information;
- *As you direct or consent:* We may use and disclose personal information when you direct or instruct us to do so, or otherwise provide your consent (for example: when you choose to include personal information in materials you upload to the Services, or when you include personal information in a support request to us);
- *To enable and transmit social media messages:* We may use and disclose personal information to enable and transmit social media messages via the Services (for example: when an End User uses the Services to publish a communication to Facebook, Twitter, and other social media channels);
- *To enable and transmit email messages:* We may use and disclose personal information to enable and transmit email messages via the Services (for example: when a School uses the Services to send an email message to students);
- *To enable and transmit SMS/MMS/Mobile messages:* We may use and disclose personal information to enable and transmit SMS/MMS and other mobile messages via the Services (for example: when a School uses the Services to send an SMS message to parents and guardians);
- *To enable and transmit voice and VOIP messages:* We may use and disclose personal information to enable and transmit voice/VOIP and other audible messages via the Services (for

example: when a School uses the Services to send a voice message to parents and guardians);

- *To maintain security and availability of the Services:* We may use and disclose personal information to ensure the security and availability of the Services (for example: when we perform system and database evaluations and tests);
- *For legal purposes:* We may use and disclose personal information (i) to comply with applicable laws, regulations, court orders, legal processes, or to respond to any government, agency, or regulatory request, (ii) to detect or otherwise manage fraud, security, or technical issues, (iii) to protect the safety, rights, or property of any person, the public, or Apptegy, or (iv) to enforce our rights arising from agreements with Clients and Users, including our Terms of Use, and for billing and collection purposes;
- *To contact you about Services:* If you are a School or a teacher or staff member with a School-Created User Account, we may use and disclose personal information to contact you about other Apptegy Services that may be of interest to you. We will not contact School-Created User Accounts that we know are parents, guardians, or students about other Apptegy Services;
- *To contact you about resources and events:* If you are a School or a teacher or staff member with a School-Created User Account, we may use and disclose personal information to contact you about other Apptegy resources and events that may be of interest to you (for example: webinars and the publication of new educational materials). We will not contact School-Created User Accounts that we know are parents, guardians, or students about other resources or events;
- *For account servicing and maintenance:* We may use and disclose personal information to help us service, maintain, and support User accounts (for example: billing or technical support, and product updates);
- *To measure and improve client engagement:* We may use and/or disclose personal information to help us measure and improve engagement with Users (for example: we use Google Analytics to help us understand how our users use our Services – you can read more about how Google uses our information here: <https://www.google.com/intl/en/policies/privacy/> and you can also opt-out of Google Analytics here: <https://tools.google.com/dlpage/gaoptout>; we also use Pendo to help us understand how our users use our Services – you can read more about how Pendo uses our information here: <https://www.pendo.io/legal/privacy-policy/>); and
- *For corporate business purposes:* We may use and disclose personal information (a) to our current or future parent company, affiliates, subsidiaries, and other companies under common control and ownership, or (b) to a buyer or other successor in connection with, or during negotiations for, a merger, acquisition, reorganization, or other sale or transfer of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding.

We may use and disclose personal information with and to third parties when it is necessary to provide the Services or for our business (for example: to complete any of the foregoing activities;

or when we need to process payments from Clients; or when we translate content that includes personal information from English into other languages; or when we comply with appropriate security standards). When we use and disclose personal information with third parties, the third parties are not allowed to access or use personal information of Users, unless it is needed to do their particular work with us. We will limit the personal information we provide to third parties as much as possible, and we will condition our sharing of that personal information on strict confidentiality restrictions and security instructions as often as possible.

Some examples of third parties that may receive personal information as a necessary part of providing the Services are Amazon Web Services (hosting provider), Google (communications, translations, analytics), Zoom (communications), Salesforce (Client relationship management), Pendo (analytics), AppSignal (product performance management), IMImobile (text messaging facilitator), and Intercom (Client support). For a list of third parties with whom we share personal information, please contact us by email at privacy@apptegy.com.

Please note that some personal information provided by Schools and End Users on the Services may be viewable by the public generally (for example: a School message posted on Facebook via Thrillshare Media); and some personal information provided by Schools and End Users on the Services may be viewable by other Users (for example: a message posted on a group message via Thrillshare Rooms where other School-Created User Accounts in the Room have permission to view). As explained above, Schools and End Users under School-Created User Accounts make those choices and are responsible for them.

When we use and/or disclose personal information for legal purposes or in connection with our corporate business purposes, we will limit the personal information we provide as much as possible, and we will condition our sharing of that personal information on strict confidentiality restrictions and security instructions as often as possible.

Please note that we will not use or disclose information (whether personal or otherwise) about individual students collected from Schools or School-Created User Accounts for the purpose of commercial marketing or targeted advertising.

We may use and disclose anonymized or generalized (non-identifiable) aggregated information with third parties for various reasons, including to promote and improve our Services. In these circumstances, we will take appropriate measures to de-identify (and prevent any party from re-identifying) any information used or disclosed in this way.

4. ADVERTISING AND MARKETING; TRACKING; OPT-OUT

As explained above, if you are a School or a teacher, administrator, or staff member under a School-Created User Account, we may use your information for limited advertising and marketing

purposes, including to contact you about Services that we believe may be of interest to you, and to promote other Apptegy resources and events. We will not contact End Users that we know are parents, guardians, and students with respect to the foregoing.

Our marketing communications will include instructions for how to opt-out of these communications or change your communication preferences. You may also contact us by email at privacy@apptegy.com to manage your marketing communication preferences at any time. Please note that certain information is required to use parts of the Services as intended (for example: to receive the communications sent by your School).

Please note that End User accounts are controlled and managed by the Client that added the End User to the Services (for example: the School that is your employer or that you attend as a student). In some instances, End Users that want to manage, change, disable, or deactivate their account or account preferences must contact the Client that invited or added them to the Services. Please see our Terms of Use for more information.

We use cookies, beacons, and other similar tracking technologies. These are small text files containing an identifier (a string of letters and numbers) that are sent by a website server to your browser when you visit a website and are stored in your browser. We only use these technologies for the purpose of providing and improving our Services for our Users. A few examples include: we use cookies that are necessary for the Services to function (for example: to remember your cookie preferences), to personalize the Services and to recognize you when you return to the Services (for example: to remember your language preferences), to help us measure and improve engagement with Users (for example: to analyze the usage trends and patterns for our different products), and to promote Services that we believe may be of interest to you. We do not use the technologies for third party targeted marketing or advertising purposes. In some cases, you may manage the use of cookies for our Services by adjusting your individual browser settings. You may learn more about managing cookies here: <https://www.aboutcookies.org/>. Please note that our Services do not currently process “do not track” features offered by some browsers and devices. Please also note that if you do not allow certain cookies, then the Services may not function properly.

We will not use or disclose information (whether personal or otherwise) about individual students collected from Schools or School-Created User Accounts for the purpose of commercial marketing or targeted advertising.

5. CALIFORNIA PRIVACY NOTICE

This California Privacy Notice describes how we as a business collect, use, disclose, and otherwise process personal information of individual residents of the State of California within the scope of the California Consumer Privacy Act of 2018 (“**CCPA**,” as amended by the California Privacy Rights Act of 2020, and its implementing regulations).

This California Privacy Notice applies only to individual users of our Services who are residents of the State of California, and only where we act as a “business” with or for that individual. For example, this section may apply for California residents who use our Services as a Visitor. For applicable Users, this section is a supplement to the other parts of this Policy.

However, if you are an End User using the Services under a School-Created User Account, this section does not apply to you because we do not act as a business with or for individual End Users. In these instances, as explained in more detail in section 2 above, the privacy and security policies of your School govern your personal information and your rights. Even though this section does not apply to individual End Users, below we have included the categories of personal information that might be collected at the direction of your School. Not all categories will be collected or received for every End User. We are providing this extra information as a courtesy and for information purposes only, and it does not change our obligations under the CCPA. As explained in section 2 above, personal information of End Users is under the direct control of the School, and we only collect End User personal information that is reasonably necessary to provide the Services requested by the Client.

As explained above, we collect limited personal information about individual Users with whom we have a direct “business” relationship. Not all categories will be collected or received for every individual. Under these circumstances, we may collect or receive (and may have collected or received during the 12-month period prior to the effective date of this Privacy Policy) the following categories of personal information:

- *Identifiers.* Apptegy collects identifiers (for example: name, address, phone number, email address, and other similar identifiers) from you, from your device or browser, and from our third party business relationships. For End Users, identifiers may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Online activity and device information.* Apptegy collects online activity and device information (for example: IP address, browser and device data, browsing history, search history, usage data, analytics information) from you, from your device or browser, and from our third party business relationships. For End Users, online activity and device information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Communications.* Apptegy collects communications (for example: content of communications with us, “contact us” submissions, emails, logs) from you, from your device or browser, and from our third party business relationships. For End Users, communications may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Geolocation.* Apptegy collects general geolocation information (for example: location data from device or IP address) from you, from your device or browser, and from our third party business

relationships. For End Users, general geolocation may be collected at the direction of your School depending on the Services being used by your School and its End Users. We do not collect precise geolocation.

- *Biometric information.* Apptegy does not collect biometric information (for example: hair color, height, voice, facial recognition). For End Users, verification data from your device provider and/or browser may be collected at the direction of your School depending on the Services being used by your School and its End Users to authenticate your login to the Services under the School's account.
- *Characteristics of protected classifications under CA law.* Apptegy does not collect characteristics of protected classifications (for example: age, race, gender, disability). For End Users, protected classification information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Employment or professional information.* Apptegy does not collect employment or professional information (for example: your School employer). For End Users, employment or professional information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Audio, visual, or similar sensory information.* Apptegy collects audio, visual, or similar sensory information (for example: photographs, voice and video recordings of calls with us (where permitted by law)) from you. For End Users, audio, visual, or similar sensory information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Commercial information.* Apptegy collects commercial information (for example: information related to Services you have accessed or purchased, purchasing history and tendencies) from you, from your device or browser, and from our third party business relationships. For End Users, commercial information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Other personal information.* Apptegy collects other personal information (for example: any information about you that is included in user generated content) from you, from your device or browser, and from our third party business relationships. For End Users, other personal information may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Inferences.* Apptegy collects inferences (for example: information that could be used to create a user profile reflecting your preferences, attitudes, behavior, and similar characteristics) from you, from your device or browser, and from our third party business relationships. For End Users, other inferences may be collected at the direction of your School depending on the Services being used by your School and its End Users.
- *Financial information.* Apptegy does not collect financial information (for example: credit card and debit card numbers, account numbers) except for Client payment information. For End

Users, financial information may be collected at the direction of your School depending on the Services being used by your School and its End Users.

- *Sensitive personal information.* Sensitive personal information (for example: social security numbers and other government-issued identifiers; precise geolocation) is not collected.

Please also see section 2 above for more information about the personal information we collect. We may in some instances collect personal information other than what is set out in the table above (for example: for legal purposes or when you include information in communications with us that we don't ordinarily collect).

We may use your personal information for the purposes described in section 3 above (How We Use and Disclose Your Information). This includes:

- To provide and operate our Services;
- As you direct or consent;
- To maintain security and availability of the Services;
- For legal purposes;
- To contact you about Services, resources and events (we will not contact School-Created User Accounts that we know are parents, guardians, or students);
- For account servicing and maintenance;
- To measure and improve client engagement; and
- For corporate business purposes.

Please see section 3 above for additional information.

As also discussed in section 3 above, we may disclose personal information to the following categories of third parties for a business purpose:

- *Our third party vendors to provide, promote, or improve our Services.* We may use and disclose personal information with third parties when it is necessary to provide the Services or for our business (for example: when an End User uses the Services to post a social media, SMS, email, or voice communication that includes personal information; or when we need to process payments from Clients; or when we translate content that includes personal information from English into other languages; or when we need help to ensure compliance with appropriate security standards).
- *Social media messaging vendors who enable the delivery of social media messages.* We may use and disclose personal information with third parties to enable and transmit social media messages via the Services.

- *Email vendors who enable the delivery of email messages.* We may use and disclose personal information with third parties to enable and transmit emails via the Services.
- *Mobile messaging vendors who enable the delivery of mobile messages.* We may use and disclose personal information with third parties to enable and transmit SMS/MMS/Mobile messages via the Services.
- *Voice/VOIP and other audible messaging vendors who enable the delivery of voice/VOIP and audible messages.* We may use and disclose personal information with third parties to enable and transmit voice/VOIP and audible messages via the Services.
- *Third parties at your direction.* We may use and disclose personal information with third parties at your direction or with your consent (for example: third parties you choose to interact with via the Services).
- *Third party analytics and performance vendors.* We may use and disclose personal information with third parties to measure and improve client engagement (for example: we use Google Analytics and Pendo to help us understand how our users use the Services).
- *Third party security and technology vendors.* We may use and disclose personal information with third parties for servicing and maintaining the Services (for example: to help us with security measures, billing, or technical support).

Please also see section 3 above for more information about how we may disclose personal information. We may in some instances disclose personal information with third parties for other purposes than what is set out in the table above (for example: in connection with our corporate business purposes or for legal purposes).

Please note that we do not sell or otherwise attempt to monetize your personal information with third parties. However, under the CCPA, some of our activities may be considered “sales” of information or cross-context behavioral advertising . For example, we may disclose “identifiers” (see above) with our third party business partners, or use tracking technologies as described above, to help us promote Apptegy and our Services to Users that are Visitors. We do not promote Apptegy or our Services through cross-context behavioral advertising to End Users and School-Created User Accounts (for example: students, parents, and guardians).

Please note that, as stated above, we will not sell or share personal information about individual consumers under the age of legal majority for the purpose of commercial marketing or targeted advertising. For more information about our practices and policies for children’s personal information, please see section 8 below and our Terms.

For more information about our California Student Privacy Certification for practices relating to the personal information of children, please see section 8 below.

We keep the personal information we collect about you for as long as is needed and appropriate for your use of the Services as set out in our Terms and this Privacy Policy. We dispose of the information we collect in accordance with our data retention policies and procedures. Please see section 9 below for more information.

If you are a qualifying California resident under CCPA, we provide the following rights with respect to your personal information when we act as a “business” with or for you (subject to certain limitations in the CCPA):

- *Right to know.* Upon verifiable request we will provide you with the following information about your personal information over the prior 12 months: (1) the specific pieces and categories of personal information we have collected about you; (2) the categories of sources from which we have collected your personal information; (3) our business purposes for collecting, selling, and sharing your personal information; (4) the categories of third parties with which we have shared your personal information; (5) the categories of personal information we have disclosed about you for a business purpose; and (6) if applicable, categories of personal information we have sold or shared about you, and the categories of third parties to which the personal information was sold or shared, for cross-context behavioral advertising.
- *Right to delete.* Upon verifiable request we will delete personal information we have collected about you and will direct our service providers to do the same, subject to certain exceptions in the CCPA.
- *Right to opt out of sales and sharing to third parties for cross-context behavioral advertising.* We do not sell your personal information to third parties. Notwithstanding that, you have the right to direct us to not sell or share your personal information to third parties for cross-context behavioral advertising. In addition, we have provided our users with a link to submit this request, found here: www.apptegy.com/donotsellmypersonalinformation. Please note that if you are not logged into an account when you submit an opt-out request, your request will only be associated with the that browser. Please also note that if you opt-out from cross-context behavioral advertising, you may still receive ads about Apptegy but they will not be tailored to you.
- *Right to correct.* Upon verifiable request we will correct any personal information that we have collected about you that is incorrect.
- *Limit use and disclosure of sensitive personal information.* We do not collect sensitive personal information. Notwithstanding that, you have the right to limit our use and disclosure of sensitive personal information to certain purposes in accordance with the CCPA.
- *Right to not be subject to discrimination for enforcing your CCPA rights.* You will not be discriminated against by us for your exercise of CCPA rights. We will not refuse the Services, change pricing, or provide a different quality of Services because of your exercise of CCPA rights. However, please note that in some instances, exercising certain CCPA rights may cause

us to be unable to provide you with our Services because certain parts of the Services require personal information to function.

Please note, as explained above at the beginning of section 5 and in section 2.A, this section does not apply to you if you use our Services as an End User with a School-Created User Account or under an account of a School. In these instances, please contact your School about your personal information and your rights.

Please note that we will need to verify your identity before processing CCPA and other California requests, which may require us to request and obtain additional information from you. To do so, we may ask that you provide us with your first name, middle name, last name, email address, phone number, and address. We may also ask you to provide answers to questions about yourself to help verify your identity. We may also use or rely on third-party identity services to help us with identification verification and defend against fraudulent requests. We will use that information only to review and address your requests. We reserve the right to decline or limit requests in certain circumstances – for example, when we are unable to verify your identity or locate information in our systems, or when you have previously made two CCPA requests in the prior 12 months, or as otherwise permitted by applicable law.

You may designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise your CCPA and other California rights. Before accepting such a request from an agent, we will require the agent to provide us with proof that you have authorized it to act on your behalf, and we may also need you to verify your identity directly with us.

Please note that we will also comply with valid requests from California residents that have an established business relationship with us under California’s “Shine the Light” law.

We do not provide financial incentives related to the collection, use, or disclosure of personal information.

If you have questions, or would like to exercise any of your rights under the CCPA, please contact us at any of the following:

- By email at privacy@apptegy.com;
- By telephone at 1-888-501-0024; or
- By mail at Apptegy Inc., c/o Data Protection Officer, 2201 Brookwood Drive, Suite 115, Little Rock, AR 72202.

6. EUROPEAN UNION AND UNITED KINGDOM PRIVACY NOTICE

If you are an individual resident of the European Union or the United Kingdom, you have certain rights with respect to your personal information, including under the General Data Protection Regulation (“**GDPR**”) and the GDPR as transposed into the law of the United Kingdom (“**UK GDPR**”). This includes, among other rights, the right to be informed and request access to the personal information about you that we have collected via our Services. You may also have the right to ask that your personal information be corrected, updated, or deleted.

Please note that we will comply with valid requests from residents of the European Union and the United Kingdom subject to relevant legal exemptions. Please also note that we will need to verify your identity before processing any such requests, which may require us to request and obtain additional information from you. We will use that information only to review and address your requests. We reserve the right to decline or limit requests in certain circumstances – for example, when we are unable to verify your identity or locate information in our systems, or as otherwise permitted by applicable law.

You may designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise your rights under this section. Before accepting such a request from an agent, we will require the agent to provide us with proof that you have authorized them to act on your behalf, and we may also need you to verify your identity directly with us.

If you use our Services under an account of a School, please contact your School about your personal information and your rights. Otherwise, if you have questions, or would like to exercise any of your rights under the GDPR, UK GDPR, or any similar right, as an individual user under an individual account, please contact us, care of our Data Protection Officer, at any of the following:

- By email at privacy@apptegy.com;
- By telephone at 1-888-501-0024; or
- By mail at Apptegy Inc., c/o Data Protection Officer, 2201 Brookwood Drive, Suite 115, Little Rock, AR 72202.

You may also contact the data protection authority of your jurisdiction.

7. CANADIAN RESIDENTS

If you are a Canadian resident, this section applies to you.

Consent: By submitting personal information to us, or our service providers and agents, you consent to the collection use, disclosure, and transfer of your personal information in accordance with this Privacy Policy and as permitted or required by law. You may withdraw your consent at any time to the collection, use, disclosure, or transfer of your personal information time by contacting

us at privacy@apptegy.com. If you withdraw your consent (or if you decide not to provide certain personal information), you acknowledge that we may not be able to provide you, or continue to provide you, with certain products, services, or information that may be of value to you.

Retention of Personal Information: The personal information that you provide will be retained by us in accordance with applicable laws. However, we will take reasonable steps to destroy or permanently de-identify personal information we hold if it is no longer needed for the purposes for which it was collected.

Access and Correction: We will take reasonable steps to ensure the personal information we hold is accurate, complete and up-to-date. Upon your written request, and subject to certain exceptions provided by law, we will inform you of the existence, use, and disclosure of your personal information and give you access to that information. We may charge a minimal fee for providing such access to you. If you believe that the personal information that we hold about you is not accurate or complete, you may write to us at privacy@apptegy.com. If you are able to establish that the information is not accurate or complete, we will take reasonable steps to delete and/or correct the information so that it is accurate, complete, and up-to-date. In order to facilitate a request to correct or update information, we may ask you to provide additional information to confirm your identity. Any such information will only be used for the purpose of confirming your identity and will not be retained by us.

Interest-Based Advertising: To opt-out of interest-based advertising, and to find information about how to block or limit cookies, visit [AdChoices](#), the Canadian self-regulatory program for online interest-based advertising, administered by the Digital Advertising Alliance of Canada (“**DAAC**”).

Canada’s Anti Spam Law (“**CASL**”)

We will only send you commercial electronic messages (“**CEMs**”) where we have your express or implied consent to do so. Your consent to receive CEMs is implied where we have an existing business relationship with you, or you have reached out to us and made an inquiry within a certain time frame. You may unsubscribe from receiving CEMs at any time, by clicking the unsubscribe button on an email or following the direction provided in a text message. This paragraph only applies to CEMs that are sent by Apptegy on its own behalf. CEMs sent by customers using the Services are the sole responsibility of the particular customer.

8. CHILDREN’S AND STUDENT DATA PRIVACY

Protecting children’s and students’ privacy is especially important to us. We participate in the iKeepSafe COPPA Safe Harbor program. We have been granted the iKeepSafe COPPA Safe Harbor seal signifying that our Site and Thrillshare, as well as the software that runs the Site and Thrillshare, have been reviewed and approved for having policies and practices surrounding the

collection, use, maintenance, and disclosure of personal information from children consistent with the iKeepSafe COPPA Safe Harbor program guidelines. COPPA protects the online privacy of Children under the age of 13.

We also participate in the iKeepSafe FERPA Certification and California Student Privacy Certification programs. We have been granted the iKeepSafe FERPA Certified seal and the California Student Privacy Certification seal signifying that our Site and Thrillshare, as well as the software that runs the Site and Thrillshare, have been reviewed and approved for having policies and practices surrounding the collection, use, maintenance, and disclosure of personal information from children consistent with the iKeepSafe FERPA Certification and California Student Privacy Certification program guidelines.

For additional information please visit <https://ikeepSAFE.org/certifications/> or email IKeepSafe Safe Harbor program at privacy@ikeepSAFE.org.

We do not intentionally request, collect, store, or use personal information from or about any child under the age of legal majority for our own use. We only request, collect, store, and use personal information about children as is necessary to provide the Services to our Clients and Users, and only as requested by the Client, as explained more fully in this Policy and in our Terms of Use. If we learn that we have unintentionally collected personal information from or about a child other than as set out in this Policy and in our Terms of Use, we will delete that information as soon as reasonably practicable. Please see our Terms of Use for more information about the limited circumstances when children may use the Services.

As explained above, our Clients are often Schools. In providing the Services to Schools we may receive student data from or about children as a necessary part of providing the Services to the Client. We may receive student data from a School directly (for example: student data about the students attending the School) or from End Users using our Services under a School-Created User Account (for example: a teacher, student, parent, or guardian using the Services set up by their School). The student data we receive may include educational records and other personal information about students. When we receive student data in connection with providing the Services for a Client, we collect, use, and maintain it under the direct control of the Client and only as is necessary to provide the Services requested by the Client and its End Users. Apptegy does not disclose student information to third parties except as reasonably necessary to support the internal operations of the Services, as further set out in Section 3 above.

Please see Section 2.A above (Personal Information from Schools and Under School Accounts) for more information about student information provided by and collected from Schools and End Users using Services under a School account, including children under the age of 13.

If you are an End User using the Services under a Client account (for example: a student, parent, or guardian using a School-Created User Account), and you have questions or requests about the personal information of a student or want to review the personal information of a student that has been collected by Apptegy, please contact your School directly.

Apptegy respects and values the privacy of student data, and we work hard to protect it. When a law or regulation creates direct obligations for Apptegy about student data privacy, we comply with it. For example, Apptegy collects, uses, and maintains student data in accordance with the Family Educational Rights and Privacy Act (“**FERPA**”) and the Children’s Online Privacy and Protection Act (“**COPPA**”), and only as is set out in this Policy and the Terms of Use. When a law or regulation creates obligations for a Client about student data privacy, we work with the Client to allow the Client to comply. For example, through the Services, Apptegy collects, uses, and maintains student data under the direct control of the Client as is required under FERPA.

Without limiting the generality of the foregoing, Apptegy relies on the Client to obtain the required legal consents from End Users invited or added to the Services by the Client, including parents, guardians, and students. Our Clients consent, as agents for and on behalf of the children, parents, and guardians invited or added to the Services by the Client, to Apptegy’s collection, use, and storage of personal information about or from the children. We rely on our Clients’ consent per the previous sentence for the purposes of complying with COPPA, and we are authorized to presume that Clients have obtained and will maintain all required parent or guardian consent for Apptegy’s collection, use, and disclosure of information for any children under the age of thirteen (13) that are invited or added to the Services under Client accounts. This is because, as explained above, our Clients are the Schools; we do not have direct relationships with individual End Users of the Services. As such, if you are a School and invite or add children to use the Services under your Client account, or if you allow the End Users under your account to provide personal information for or about children, you represent and warrant that you are consenting as agents for and on behalf of your End Users (as set out above) or have obtained and will maintain all required consents from students, parents, and guardians, as applicable, for Apptegy’s collection, use, and storage of personal information from or about any children under your account, including children under the age of thirteen (13).

PLEASE NOTE that some or all of the information we collect about or from End Users may not be private as to the individual User. For example, for Users of Rooms, information shared by a User via a message feature 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 this Privacy Policy and our Terms.

PLEASE NOTE while many parts of the Services do not require personal information to function as intended, and we will not collect more personal information than is reasonably necessary to support the internal operations of the Services, we encourage parents and guardians to monitor their child's use of the Services, particularly Rooms, and to assist us by instructing them to never provide personal information on the Services, particularly including Rooms, without your permission.

PLEASE NOTE that if you discover or are made aware of any activity or information on the Services that is or may be connected to the abduction or sexual exploitation of a child, you should contact law enforcement authorities immediately. Please see the National Center for Missing and Exploited Children (NCMEC) (www.missingkids.org/education) for more information and resources related to abduction and child sexual exploitation prevention.

As discussed above, we may use and disclose personal information with and to third parties when it is necessary to provide the Services or for our business. For a list of third parties with whom we share student data or child personal information, please contact us by email at privacy@apptegy.com or visit www.apptegy.com/privacy-policy/service-providers.

9. SECURITY OF INFORMATION; DATA TRANSFERS AND RETENTION

Personal information is very important to us, and we continuously work to keep it secure and to improve our practices. We maintain administrative, technical, and physical controls and practices that we believe are reasonable to safeguard against the unauthorized access and use of personal information. For example, we conduct periodic system evaluations, maintain system and security certifications, manage and log system access, and perform and maintain regular backups. We use industry-accepted encryption practices to protect personal information during transfer and at rest. Our employees and contract personnel receive privacy and security training, and are bound by our personal information policies. Finally, we work to stay informed about industry requirements and changing standards. Notwithstanding the foregoing, we cannot and do not guarantee the total security of your information in all circumstances.

If we become aware of a security incident, we will comply with applicable law. We will notify impacted Clients of verified security incidents as soon as practicable, and respond to them, in accordance with your Client Agreement (as defined in the Terms of Use) and applicable law. If you are an impacted End User (for example: a teacher, staff, student, parent, or guardian added to the Services by a School), we will notify you of verified security incidents, and respond to them, in accordance with the instructions of the Client that added you to the Services (for example: the School that is your employer or that you attend as a student) and applicable law. If you are an impacted Visitor and you do not use the Services as an End User (for example: an individual browsing a public part of the Sites that does not require a log-in or an invitation from a Client), we will notify you of verified security incidents, and respond to them, in accordance with applicable law.

We are based in the United States. Your information will be accessed, transferred, processed, and stored in the United States. We also have offices and personnel in locations outside of the United States, including Mexico. In some circumstances your information may be accessed, transferred, processed, or stored outside of the United States when that is reasonably necessary to provide, operate, or maintain the Services (for example: to process information updates for School-Created User Accounts; or to provide maintenance and support for parts of the Services). We maintain administrative, technical, and physical controls and practices that we believe are reasonable to safeguard the access, transfer, processing, and storage of personal information in and to all locations where we do business. By using the Services, or providing us with any information, you are consenting to the access, transfer, processing, and storage of your information, including personal information, in the United States and in the other locations where we do business.

How we retain and delete personal information from or about you depends on our relationship with you. Specifically:

- If you are a Client (for example: a School), we will retain and delete personal information we collect from or about you and your End Users according to your instructions, and in accordance with your Client Agreement (as defined in the Terms of Use) and applicable law. When you are no longer a Client (for example: if your Client Agreement ends), we will delete personal information associated with your Client account in accordance with your Client Agreement and applicable law, and as soon as reasonably practicable after the termination of your Client relationship. If you are a Client and have questions or requests about retaining or deleting personal information associated with your Client account, please contact us by any of the methods set out below in the section 10 titled “Contact Us”; or
- If you are an End User (for example: a teacher, staff, student, parent, or guardian added to the Services by a School), we will retain and delete personal information from or about you according to the instructions of the Client that added you to the Services (for example: the School that is your employer or that you attend as a student) and applicable law. If you are an End User and have questions or requests about retaining or deleting personal information under your School’s Client account or your School-Created User Account, please direct those questions and requests directly to your School. If you contact us regarding these questions and requests, we will direct them to your School; or
- If you are a Visitor and you do not use the Services as an End User (for example: an individual browsing a public part of the Sites that does not require a log-in or an invitation from a Client), then we may retain personal information we collect pursuant to this Policy for as long as permitted under applicable law. If you are a Visitor and have questions or requests about retaining or deleting personal information associated with you, please contact us by any of the methods set out below in the section 10 titled “Contact Us.”

10. CONTACT US

If you have questions about our policies or any related matter, please contact us at any of the following:

- By email at privacy@apptegy.com;
- By telephone at 1-888-501-0024; or
- By mail at Apptegy Inc., c/o Data Protection Officer, 2201 Brookwood Drive, Suite 115, Little Rock, AR 72202.

11. THIRD PARTY FUNCTIONALITY AND TOOLS

We use third party providers for various aspects of our Services. For example, Schools (or End Users under School-Created User Accounts) may use the Services to post a communication to a Facebook or Twitter account, or to translate a communication from English to another language. In addition, there may be links or references on our Services to products and services that are offered by third parties. By using any part of the Services that incorporates or is made available by a third party, you will also be subject to the third party practices and policies associated with the third party services that you use. **Please note that these third party practices and policies may be materially different than our practices and policies, especially with respect to privacy and security.** Please note that we are not responsible for the practices and policies of any third party, including privacy and security practices and policies. If you choose to access or use any third party product or service, you do so at your own risk.

For additional information about our third party providers and partners, please see our Terms of Use, accessible at www.apptegy.com/terms-and-conditions.

12. MISCELLANEOUS

We may change this Policy from time to time in our discretion. The most current version will always be at the following link: <https://www.apptegy.com/privacy>. We encourage you to review it regularly. Any changes will be effective immediately upon us posting the updated Policy. If we make updates or changes, we will give notice by updating the posted date for this Policy. In some cases and in our sole discretion, we may provide additional notice (for example: by a pop-up or banner notice on the Services, or by sending you an email notification). By continuing to use the Services after changes are effective, you will be bound by the revised Policy. If you do not agree with any updates to the Policy, you may not continue to use the Services. Notwithstanding the foregoing, if we make updates or changes that materially change User rights with respect to personal information, or reduce the level of protection for personal information, we will comply with applicable law. We will provide you with advance notice on the Services and, if required by applicable law, request your consent. For impacted Clients, we will also provide notice to you via the contact information you

have provided to us. Please return to this page periodically to ensure you are familiar with the most current version of the Policy.

Please feel free to contact us with respect to any question about this Privacy Policy at:

- 1-888-501-0024
- privacy@apptegy.com
- Apptegy, Inc., 2201 Brookwood Drive, Suite 115, Little Rock, Arkansas 72202

Effective: May 31, 2023



CERTIFICATE OF LIABILITY INSURANCE

6/14/2024

DATE (MM/DD/YYYY)

6/6/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Lockton Companies
1185 Avenue of the Americas, Suite 2010
New York NY 10036
646-572-7300

CONTACT NAME:
PHONE (A/C, No, Ext):
FAX (A/C, No):
E-MAIL ADDRESS:

INSURED 1543174 Apptegy, Inc
2201 Brookwood Dr, Ste 115
Little Rock, AZ 72202

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A : Transportation Insurance Company	A	20494
INSURER B : The Charter Oak Fire Insurance Company	A++	25615
INSURER C : The Continental Casualty Company	A	20443
INSURER D : The Continental Insurance Company	A	35289
INSURER E : QBE Insurance Corporation	A	39217
INSURER F : Lloyd's Syndicate 3624	NR	

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	COMMERCIAL GENERAL LIABILITY CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:		<input checked="" type="checkbox"/>	7039620112	5/30/2024	5/30/2025	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 15,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
B	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS NON-OWNED AUTOS ONLY			7039620126	5/30/2024	5/30/2025	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ XXXXXXXX BODILY INJURY (Per accident) \$ XXXXXXXX PROPERTY DAMAGE (Per accident) \$ XXXXXXXX \$ XXXXXXXX
D	UMBRELLA LIAB EXCESS LIAB DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			7039620157	5/30/2024	5/30/2025	EACH OCCURRENCE \$ 15,000,000 AGGREGATE \$ 15,000,000 \$ XXXXXXXX
D	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below			7039620143	5/30/2024	5/30/2025	PER STATUTE OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
C F E	Crime Cyber/Tech E&O Professional			752301394 MPL4853522.23 00037211PIC	5/22/2023 6/18/2023 6/14/2023	9/4/2024 6/18/2024 6/14/2024	Limit: \$1M Ded: \$5K Limit: \$3M Ret: \$10K PL \$1M Cyber: \$500K EL: \$10M

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
[Signature]



STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0)

School Board of Clay County

and

Apptegy, Inc.

Provider Name

Version: 1r7

© 2021 Access 4 Learning (A4L) Community. All Rights Reserved.

This document may only be used by A4L Community members and may not be altered in any substantive manner.

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

School Board of Clay County, located at 900 Walnut Street, Green Cove Springs, FL 32043
(the “**Local Education Agency**” or “**LEA**”)

And Aptegy, Inc. located at 2201 Brookwood Dr., Ste. 115, Little R (the “**Provider**”).
Provider Name Street, City, State

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA 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**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check Box if Required**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”**. (Optional)
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit “E”** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Ethan Caren Title: Director of Information Services

Address: 900 Walnut Street, Green Cove Springs, FL 32043

Phone: 904-336-9603 Email: ethan.caren@myoneclay.net

The designated representative for the Provider for this DPA is:

Name: Jack Easterly Title: Director of Legal

Address: 2201 Brookwood Dr., Ste. 115, Little Rock, AR 72202

Phone: 501-613-0370 Email: legal@apptegy.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA, School Board of Clay County

By: _____ Date: 07/15/2024

Printed Name: Ethan Caren Title/Position: Director of Information Services

Apptegy, Inc.

Name of Provider

By:  Date: 7/16/24

Printed Name: Robert Butler Title/Position: Chief Executive Officer

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit “A”** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between

Exhibit “H”, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit “H”** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law: Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider 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 DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Vendors/Providers - please list all applications you support that are in use at the District, describe what your application does and what grade levels and/or staff groups will access your software (as applicable).

Access to Provider's software-as-a-service platform for distributing communication across multiple outlets including integrated website and mobile app.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input checked="" type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input checked="" type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input checked="" type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input checked="" type="checkbox"/>
	Year of graduation	<input checked="" type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input checked="" type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input checked="" type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input checked="" type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input checked="" type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input checked="" type="checkbox"/>
	Student course data	<input checked="" type="checkbox"/>
	Student course grades/ performance scores	<input checked="" type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application: Please see Exhibit H for more information.	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “Student-Generated Content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

School Board of Clay County Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Categories of data

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Describe here or attach special instructions

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By Date:

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Clay County District Schools ("Originating LEA") which is dated _____ to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Apptegy, Inc. _____

Name of Provider

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between School Board of Clay County (Originating LEA) and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____ Title: _____

Address: _____

Telephone Number: _____ Email: _____

EXHIBIT “F”**DATA SECURITY REQUIREMENTS****Adequate Cybersecurity Frameworks****2/24/2020**

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* (“Cybersecurity Frameworks”) that may be utilized by Provider.

Cybersecurity Frameworks

Check those that apply	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input checked="" type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"**Supplemental SDPC State Terms for [State]**Version 1

Providers/Operators are to comply with the Florida Student Online Personal Information Protection Act, Florida Statute 1006.1494. This Act (effective 7/1/2023 and initiated from SB 662 in 2023) establishes new and different terms than those outlined in the National Student Data Privacy Agreement contained herein. Providers/Operators are subject to all of the Act's privacy terms, including, but not limited to the following:

1) An operator may not knowingly do any of the following:

a) Engage in targeted advertising on the operator's site, service, or application, or targeted advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, which the operator has acquired because of the use of that operator's site, service or application for K-12 school purposes.

b) Use covered information, including persistent unique identifiers, created, or gathered by the operator's site service, or application to amass a profile of a student, except in furtherance of k-12 school purposes.

c) Share, sell, or rent a student's information, including covered information

2) An operator shall do all the following:

a) Collect no more covered information that is reasonably necessary to operate an Internet website, online service, online application, or mobile application....

b) Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information which are designed to protect it from unauthorized access destruction, use, modification, or disclosure.

c) Unless a parent or guardian expressly consents to the operator retaining a student's covered information, delete the covered information at the conclusion of the course, or corresponding program and no later than 90 days after a student is no longer enrolled in a school within the district, upon notice by the school district.

EXHIBIT "H"**Additional Terms or Modifications**

Version _____

LEA and Provider agree to the following additional terms and modifications:

(This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None." 618-1/4715859.1)

1. The Parties acknowledge and agree that the rights and obligations of the LEA and Apptegy with respect to providing, accessing, and using the Services are also subject to and governed by the Apptegy Terms of Use (Terms of Use) and Privacy Policy (Privacy Policy), available as amended at the following links: <https://www.apptegy.com/terms-of-use/> and <https://www.apptegy.com/privacy-policy/>. The Terms of Use and Privacy Policy further set out how Provider will comply with its obligations under this DPA and are incorporated into this DPA in their entirety, as applicable to the LEA. In the event of a conflict between the Terms of Use, Privacy Policy, and this DPA, then this DPA shall prevail and govern.
2. The data elements selected above are those typically shared with Apptegy by its school clients. However, different clients may use different parts or features of Apptegy s services, and an individual client s use of Apptegy s services may change over time. In such case, the PII or other information that Apptegy will receive and/or access in order to provide its services may change or be supplemented. Additionally, not all of the Student Data categories selected will be shared for every student. Which data elements Apptegy may have access to is under the control of a client. If a guardian, student, or other individual wishes to review a list of PII accessed by Apptegy, the individual should contact the applicable client to confirm.
3. Article VII, section 7 is replaced in its entirety by: "Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider 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 DPA, the Provider shall ensure that any successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement."

