Data Processing Agreement

This Data Processing Agreement dated this 19 day of April, 2023 is entered into by and between:

Freshworks Inc., a Delaware corporation with offices at 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403 ("**Freshworks**" or "**Processor**")

And Coppell Independent School District, a Texas corporation with offices at 200 S. Denton Tap Road, Coppell, TX 75019 (**"Customer" or "Controller"**)

Processor and Controller are individually referred to as "**Party**" and collectively as "**Parties**".

The Parties entered into a **Service Agreement** which requires that the Processor accesses and Processes Personal Data. This agreement together with its exhibits (together "the **Data Processing Agreement/DPA**") specify the obligations of the Parties when Freshworks is acting as Processor.

1. Scope of Contract and Distribution of Responsibilities

1..1 The Parties agree that, for Processing Personal Data, the Parties shall be Controller and Processor.

1.2 Processor shall Process Personal Data only on behalf of Controller and at all times only in accordance with this Data Processing Agreement.

1.3 Within the scope of the Service Agreement, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

2. Processing Instructions

2..1 Processor will Process Personal Data in accordance with Controller's instructions. This Data Processing Agreement contains Controller's initial instructions to Processor. The Parties agree that Controller may communicate any change in its initial instructions to the Processor by way of written notification to the Processor and that Processor shall abide by such instructions. The Processor shall maintain a secure, complete, accurate and up to date record of all such individual instructions.

2.2 For the avoidance of doubt, any instructions that would lead to processing outside the scope of this Data Processing Agreement (e.g. because a new Processing purpose is introduced) will require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the Service Agreement.

2.3 Where instructed by Controller, Processor shall correct, delete or block Personal Data.

2.4 Processor shall promptly inform the Controller in writing if, in Processor's opinion, an instruction infringes Data Protection Laws and provide an explanation of the reasons for its opinion in writing.

2.5 Processor shall not be liable for any DP Losses arising from or in connection with any processing made in accordance with Controller's instructions following Controller's receipt of any information provided by Processor in this Section 2.

3. Processor Personnel

Processor will restrict its personnel from Processing Personal Data without authorization. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

4. Disclosure to Third Parties; Data Subjects Rights

4.1 Processor will not disclose Personal Data to any third party (including any government agency, court, or law enforcement) except as set forth in this Data Processing Agreement or with written consent from Controller or as necessary to comply with applicable mandatory laws. If Processor is obliged to disclose Personal Data to a law enforcement agency or third party, Processor agrees to give Controller reasonable notice of the access request prior to granting such access, to allow Controller to seek a protective order or other appropriate remedy. If such notice is legally prohibited, Processor will take reasonable measures to protect the Personal Data from undue disclosure as if it were Processor's own confidential information being requested and shall inform Controller promptly as soon as possible if and when such legal prohibition ceases to apply.

4.2 In case Controller receives any request or communication from Data Subjects which relates to the Processing of Personal Data ("**Request**"), Processor shall provide the Controller with full cooperation, information and assistance ("**Assistance**") in relation to any such Request where instructed by Controller.

4.3 Where Processor receives a Request, Processor shall (i) not directly respond to such Request, (ii) forward the request to Controller within 3 (**three**) business days of identifying the Request as being related to the Controller and (iii) provide assistance according to further instructions from Controller.

5. Assistance

5.1 The Processor assists the Controller in ensuring compliance with the obligations by taking into account the nature of Processing and the information available to the Processor.

5.2 Where a Data Protection Impact Assessment ("**DPIA**") is required under applicable Data Protection Laws for the Processing of Personal Data, Processor shall provide upon request Controller with reasonable cooperation and assistance needed to fulfill Customer's obligation to carry out a DPIA related to Customer's use of the Services, to the extent that Customer does not otherwise have access to the relevant information and such information is available to Freshworks.

5.3 The Controller shall pay the Processor reasonable charges mutually agreed between the parties for providing the assistance in Section 5, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

6. Information Rights and Audit

6.1 Processor shall, in accordance with Data Protection Laws, make available to Controller on request in a timely manner such information as is necessary to demonstrate compliance by Processor with its obligations under Data Protection Laws.

6.2 Freshworks has obtained third-party certifications and audits set forth on our security page. Upon Controller's written request and subject to the confidentiality obligations set forth in the Service Agreement, Freshworks will make available to Controller a copy of Freshworks' then most recent third-party certifications or audits, as applicable.

6.3 Processor shall, upon reasonable notice, allow for and contribute to inspections of the Processor's Processing of Personal Data, as well as the TOMs (including data processing systems, policies, procedures and records), during regular business hours and with minimal interruption to Processor's business operations. Such inspections are conducted by the Controller, its affiliates or an independent third party on Controller's behalf (which will not be a competitor of the Processor) that is subject to reasonable confidentiality obligations.

6.4 Controller shall pay Processor reasonable costs of allowing or contributing to audits or inspections in accordance with Section 6.3 where Controller wishes to conduct more than one audit or inspection every 12 months. Processor will immediately refer to Controller any requests received from national data protection authorities that relate to the Processor's Processing of Personal Data.

6.5 Processor undertakes to cooperate with Controller in its dealings with national data protection authorities and with any audit requests received from national data protection authorities. Controller shall be entitled to disclose this Data Processing Agreement or any other documents (including contracts with subcontractors) that relate to the performance of its obligations under this Data Processing Agreement (commercial information may be removed).

7. Data Incident Management and Notification

In respect of Customer data incident Processor shall:

7.1 notify Controller of a Personal Data Breach involving Processor or a subcontractor without undue delay (but in no event later than 72 hours after becoming aware of the incident);

7.2 make reasonable efforts to identify the cause of such incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within Freshworks' reasonable control.

7.3 provide reasonable information, cooperation and assistance to Controller in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.

The obligations contained in Section 7 should not apply to data incidents that are caused by Customer or Customer's users.

8. International Data Transfer

8.1 Data that Freshworks processes for the Customer as a Processor will be processed and stored in the United States.

9. Reference the TOMS and Sub-Processors

For the Freshworks technical and organizational measures (TOMs), reference is made to and Exhibit A of this DPA.

For sub-processing, reference is made to Exhibit B of this DPA. In event of objection by the Controller to the appointment or replacement of any sub processor, Processor will either not appoint or replace the sub processor or, if this is not possible, Controller may suspend or terminate the Service(s) (without prejudice to any fees incurred by Controller prior to such suspension or termination).

10. Term and Termination

10.1 This Data Processing Agreement becomes effective upon signature. It shall continue to be in full force and effect as long as Processor is processing Personal Data shall cease automatically thereafter.

10.2 The Controller may terminate the Data Processing Agreement as well as the Service Agreement for cause, at any time upon reasonable notice or without notice, as selected by Controller, if the Processor is in material breach of the terms of this Data Processing Agreement.

10.3 Where amendments are required to ensure compliance of this Data Processing Agreements with Data Protection Laws, the Parties shall agree on such amendments upon request of Controller and, for the avoidance of doubt, with no additional costs to Controller. Where the parties are unable to agree upon such amendments, either party may terminate the Service Agreement and this Data Processing Agreement with 90 days written notice to the other party.

11. Deletion or Return of Personal Data

Controller may export all Customer Data prior to the termination of the Customer's Account. In any event, following the termination of the Customer's Account, (i) subject to (ii) and (iii) below and the Service Agreement, Customer Data will be retained for a period of 14 days from such termination within which Controller may contact Processor to export Customer Data; (ii) where the Controller does not use custom mailbox and uses the e-mail feature, if available within the Service(s), e-mails forming part of Customer Data are automatically archived for a period of 3 months; and (iii) logs are archived for a period of thirty (30) days in the log management systems, post which logs are retired to a restricted archived cold storage for a period of eleven (11) months (each a "**Data Retention Period**"). Beyond each such Data Retention Period, Processor reserves the right to delete all Customer Data in the normal course of operation except as necessary to comply with Processor's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Customer Data cannot be recovered once it is deleted.

12. Miscellaneous

12.1 In case of any conflict, the provisions of this Data Processing Agreement shall take precedence over the provisions of any other agreement with Processor.

12.2 The limitation of liability stated in the Service Agreement apply to the breach of the Data Processing Agreement.

12.3 No Party shall receive any remuneration for performing its obligations under this Data Processing Agreement except as explicitly set out herein or in another agreement.

12.4 Where this Data Processing Agreement requires a "written notice" such notice can also be communicated per email to the other Party. Notices shall be sent to the contact persons set out in the Agreement.

12.5 Any supplementary agreements or amendments to this Data Processing Agreement must be made in writing and signed by both Parties.

12.6 Should individual provisions of this Data Processing Agreement become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this agreement.

13. Definitions

"Data Protection Laws" shall mean the data protection laws of the country in which Controller is established, and any data protection laws applicable to Controller in connection with the Service Agreement. Where the Controller is not established in an EU Member State the California Consumer Privacy Act , Colorado Privacy Act, Virginia Consumer Data Protection Act, or other applicable state or federal law applies in addition.

“**DP Losses**” means all liabilities, including:

a) costs (including legal costs);

b) claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);

c) to the extent permitted by applicable law:

  i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a data protection authority or any other relevant Regulatory Authority;

  ii) compensation to a Data Subject ordered by a data protection authority to be paid by Processor;

  iii) the costs of compliance with investigations by a data protection authority or any other relevant Regulatory Authority.

"Personal Data" shall mean any information relating to an identified or identifiable natural person as defined by the applicable Data Protection Laws that is Processed by Processor as part of providing the services to Controller.

"Service Agreement" shall mean the Terms of Service available at https://www.freshworks.com/terms or a master services agreement executed between the Parties.

"Controller", **"Data Subject"**, **"Personal Data Breach"**, **"Processor"** and **"Process"/"Processing"** shall have the meaning given to them in applicable Data Protection Laws.

(CUSTOMER) **(Signature)**	DocuSigned by: Pam Sergeeff 02D1B0D593BE4D1... **(FRESHWORKS INC.)** **(Signature)**

DS

freshworks APPROVED

Name: Stephen McGilvray	**Name**: Pam Sergeeff
Title: Executive Director of Technology	**Title**: Authorized Signatory

EXHIBIT A:
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Processor maintains and enforces various policies, standards and processes designed to secure personal data and other data to which Processor employees are provided access, and updates such policies, standards and processes from time to time consistent with industry standards. Following is a description of some of the technical and organizational measures implemented by Processor as of the date of signature:

1. General Security Procedures

1.1 Processor shall be responsible for establishing and maintaining an information security program that is designed to: (i) protect the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security or integrity of the Personal Data; (iii) protect against unauthorized access to or use of the Personal Data; (iv) ensure the proper disposal of Personal Data, as further defined herein; and, (v) ensure that all employees and subcontractors of Processor, if any, comply with all of the foregoing. Processor shall designate an individual to be responsible for the information security program. Such individual shall respond to Controller inquiries regarding computer security and to be responsible for notifying Controller-designated contact(s) if a breach or an incident occurs, as further described herein.

1.2 Processor shall conduct formal privacy and security awareness training for all its employees as soon as reasonably practicable after the time of hiring and/or prior to being appointed to work on Personal Data and annually recertified thereafter. Documentation of security awareness training shall be retained by Processor, confirming that this training and subsequent annual recertification process have been completed.

1.3 Controller shall have the right to review an overview of Processor's information security program prior to the commencement of Service and annually thereafter upon Controller request.

1.4 Processor shall not transmit any unencrypted Personal Data over the internet or any unsecured network, and shall not store any Personal Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software. Processor shall encrypt Personal Data in transit into and out of the Services over public networks using industry standard protocols.

1.5 In the event of any apparent or actual theft, unauthorized use or disclosure of any Personal Data, Processor shall immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and without undue delay and within 72 hours following confirmation of any such event, provide Controller notice thereof, and such further information and assistance as may be reasonably requested. Upon Controller request, remediation actions and reasonable assurance of resolution of discovered issues shall be provided to Controller.

2. Network and Communications Security

2.1 All Processor connectivity to Controller computing systems and/or networks and all attempts at same shall be only through Controller's security gateways/firewalls and only through Controller-approved security procedures.

2.2 Processor shall not access and will not permit unauthorized persons or entities to access Controller computing systems and/or networks without Controller's express written authorization and any such actual or attempted access shall be consistent with any such authorization.

2.3 Processor shall take appropriate measures to ensure that Processor's systems connecting to Controller's systems and anything provided to Controller through such systems does not contain any computer code, programs, mechanisms or programming devices designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of Controller's systems.

2.4 Processor shall maintain technical and organisational measures for data protection including: (i) firewalls and threat detections systems to identify malicious connection attempts, to block spam, viruses and unauthorized intrusion; (ii) physical networking technology designed to resist attacks by malicious users or malicious code; and (iii) encrypted data in transit over public networks using industry standard protocols.

3. Personal Data Handling Procedures

3.1 Erasure of Information and Destruction of Electronic Storage Media. All electronic storage media containing Personal Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization, prior to departing Controller Work Area(s), with the exception of encrypted Personal Data residing on portable media for the express purpose of providing service to the Controller. Processor shall maintain commercially reasonable documented evidence of data erasure and destruction for infrastructure level resources.

3.2 Processor shall maintain authorization and authentication technologies and processes to ensure that only authorized persons access Personal Data, including: (i) granting access rights on the basis of the need-to-know-principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords that meet complexity, length and duration requirements; (iv) storing passwords in a manner that makes them undecipherable if used incorrectly or recovered in isolation; (v) encrypting, logging and auditing all access sessions to systems containing Personal Data; and (vi) instructing employees on safe administration methods when computers may be unattended such as use of password protected screen savers and session time limits.

3.3 Processor shall maintain logical controls to segregate Personal Data from other data, including the data of other customers.

3.4 Processor shall maintain measures to provide for separate processing of data for different purposes including: (i) provisioning Controller within its own application-level security domain, which creates logical separation and isolation of security principles between customers; and (ii) isolating test or development environments from live or production environments.

4. Physical Security

4.1 Processor shall ensure that at least the following physical security requirements are met:

i) All backup and archival media containing Personal Data must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by Processor. All backup and archival media containing Personal Data must be encrypted.

ii) Technical and organisational measures to control access to data center premises and facilities are in place and include: (i) staffed reception desks or security officers to restrict access to identified, authorized individuals; (ii) visitor screening on arrival to verify identity; (iii) all access doors, including equipment cages, secured with automatic door locking systems with access control systems that record and retain access histories; (iv) monitoring and recording of all areas using CCTV digital camera coverage, motion detecting alarm systems and detailed surveillance and audit logs; (v) intruder alarms present on all external emergency doors with one-way internal exit doors; and (vi) segregation of shipping and receiving areas with equipment checks upon arrival.

iii) Processor shall maintain measures to protect against accidental destruction or loss of Personal Data including: (i) fire detection and suppression, including a multi-zoned, dry-pipe, double-interlock, pre-action fire suppression system and a Very Early Smoke Detection and Alarm (VESDA); (ii) redundant on-site electricity generators with adequate supply of generator fuel and contracts with multiple fuel providers; (iii) heating, ventilation, and air conditioning (HVAC) systems that provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment and N+2 redundancy for chillers and thermal energy storage; and (iv) physical systems used for the storage and transport of data utilizing fault tolerant designs with multiple levels of redundancy.

5 Security Testing

5.1 During the performance of Services under the Agreement, Processor shall engage, at its own expense and at least one time per year, a third party vendor (“Testing Company”) to perform penetration and vulnerability testing (“Security Tests”) with respect to Processor’s systems containing and/or storing Personal Data.

5.2 The objective of such Security Tests shall be to identify design and/or functionality issues in applications or infrastructure of the Processor systems containing and/or storing Personal Data, which could expose Controller’s assets to risks from malicious activities. Security Tests shall probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to the Processor systems containing and/or storing Personal Data that could be exploited by a malicious party.

5.3 Security Tests shall identify, at a minimum, the following security vulnerabilities: invalidated or un- sanitized input; broken or excessive access controls; broken authentication and session management; cross- site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; common denial of service vulnerabilities; insecure or inconsistent configuration management; improper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

5.4 Within a reasonable period after the Security Test has been performed, Processor shall remediate the issues (if any) identified and subsequently engage, at its own expense, the Testing Company to perform a revalidation Security Test to ensure resolution of identified security issues. Results thereof shall be made available to the Controller upon request.

6. Security Audit

6.1 Processor, and all subcontracted entities (as appropriate) shall conduct at least annually an SSAE 18 (or equivalent) audit covering all systems and/or facilities utilized to provide the Service to the Controller and will furnish to Controller the results thereof promptly following Controller’s written request. If, after reviewing such audit results, Controller reasonably determines that security issues exist relating to the Service, Controller will notify Processor, in writing, and Processor will promptly discuss and where commercially feasible, address the identified issues. Any remaining issues shall be documented, tracked and addressed at such time as agreed upon by both Processor and the Controller.

Exhibit B

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

The current list of sub processors is available at https://www.freshworks.com/privacy/sub-processor/

- If Customer Data are hosted in the EEA datacentre with custom mailbox, only those services are turned on by default, where the specific sub-processor has datacentres in the EEA; however, if Controller chooses to use services like third party integrations and Apps, or Custom Apps, then data is expected to leave the EEA.
- Call recording for Freshdesk, Freshsales & Freshcaller is generated in the US, then routed to the EEA.
- Processor intends to use the service of the Freshworks group companies as sub processor. The current list of Freshworks group companies is available at https://www.freshworks.com/privacy/sub-processor/.

Exhibit C – CCPA Data Processing Addendum

This Addendum ("Addendum") forms part of the Freshworks Master Service Agreement or the Freshworks Terms of Service (in either case the"Agreement"), entered by and between Freshworks Inc. ("Freshworks" or "we") and Customer, including its subsidiaries and affiliates ("Customer" or "you"). Freshworks and Customer are each referred to herein as a "Party" and collectively as "Parties".

In consideration of the mutual obligations set forth herein, as well as those set forth in the Agreement, the Parties hereby agree that this Addendum shall be added as an addendum to the Agreement.

Please provide Freshworks with a signed copy of this Addendum, and we'll provide you a countersigned copy.

1. DEFINITIONS

1.1. All capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.2. "**Business**", "**Business Purpose(s)**", "**Commercial Purpose(s)**", "**Personal Information**", "**Service Provider**", and "**Third Party**" shall have the same meaning ascribed to such terms and phrases in the CCPA.

1.3. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

1.4. "**Process**," "**Processed**", or "**Processing**" means any operation or set of operations that are performed on Personal Information or on sets of Personal Information, whether by automated means, including the collection, use, modification, storage, disclosure and any other activity with regard to Personal Information.

1.5. "**U.S. Data Protection Laws**" means all laws and regulations of the United States of America, including the CCPA, applicable to the Processing of Personal Information (or an analogous variation of such term).

2. AMENDMENTS

2.1 **Roles**. Freshworks Processes Personal Information under the Agreement and this Addendum for the Business Purpose(s) set forth in the Agreement. For the purposes of this Addendum, Customer is a Business and Freshworks is a Service Provider

2.2 **No Sale**. Customer and Freshworks acknowledge and agree that in no event shall the transfer, disclosure, sharing, or making available of Personal Information under the Agreement and this Addendum constitute a Sale.

2.3 **Limitations on Use and Disclosure**. Freshworks is prohibited from Selling the Personal Information is receives or has made available to it under the Agreement and this Addendum. Freshworks is also prohibited from using, retaining or disclosing any Personal Information it receives or has access to under the Agreement and this Addendum for any purpose other than the specific purpose of providing the Services specified in the Agreement, and as otherwise permitted by the CCPA.

Stephen McGilvray

2.4 **Duty to Cooperate**. Freshworks will reasonably assist Customer with any consumer request to know, to delete, or to opt-out. If Freshworks receives any request from consumers, authorities, or others relating to its Processing of Personal Information, Freshworks will without undue delay inform Customer and reasonably assist Customer with developing a response (but Freshworks will not itself respond other than to confirm receipt of the request, to inform the consumer, the authorized agent or other third party that their request has been forwarded to Customer, and/or to refer them to Customer, except per reasonable instructions from Customer). Freshworks will also reasonably assist Customer with the resolution of any request or inquiries that Customer receives from governmental authorities relating to Freshworks.

2.5 **Effect of this Addendum**. In the event of any conflict or inconsistency between the terms of this Addendum and the terms of the Agreement with respect to the subject matter hereof and solely where U.S. Data Protection Laws apply, the terms of this Addendum shall control.