# CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

**IRVINE UNIFIED SCHOOL DISTRICT**

and

**JAMF Software, LLC**

**March 29, 2020**

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Irvine Unified School District (hereinafter referred to as ;'LEA") and JAMF Software, LLC (hereinafter referred to as "Provider") on March 29, 2020. LEA and Provider are each a "Party" and collectively the "Parties." This DPA is attached to and forms a part of the Service Agreement entered into by the Parties. The Parties agree to the terms stated herein.

## RECITALS

**WHEREAS,** the Provider has agreed to provide the Local Education Agency ("LEA") with certain Hosted Services ( as defined in the Service Agreement) pursuant to a contract dated March 29, 2020 ("Service Agreement"); and

**WHEREAS,** in order to provide the Hosted Services described in the Service Agreement, the Provider may receive and the LEA may provide data that is covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h. All data and information entered into the Hosted Services by the LEA is referred to in the Service Agreement as "Customer Content;" and

**WHEREAS,** the data transferred from LEAs to the Provider in connection with the provision of the Hosted Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

**WHEREAS,** if Provider will have access to Educational Records, Provider acknowledges that for the purposes of this DPA and applicable education laws, Provider will be designated as a school official with legitimate educational interests in the Educational Records provided by LEA pursuant to the Service Agreement; and

**WHEREAS,** the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

**WHEREAS,** the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Hosted Services described herein and in the Service Agreement, without the need to negotiate terms in a separate DPA.

**NOW THEREFORE,** for good and valuable consideration, the parties agree as follows:

## 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 transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In providing Hosted Services, the Provider may be considered a School Official with a legitimate educational interest, if LEA gives Provider access to Educational Records. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

**2.** **Nature of Services Provided.** The Provider has agreed to provide the following Hosted Services described below, in the Service Agreement and as may be further outlined in Exhibit "A" hereto: Hosted Services.

**3.** **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

**4.** **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 term used in the Service Agreement.

## 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. If Provider is given Student Data in connection with provision of the Hosted Services, Provider acknowledges that, for the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above.

**2.** **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of Hosted Services. To the extent the LEA is unable to respond to a parent, legal guardian or eligible student request, Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data processed by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data processed pursuant to the Hosted 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 pupil generated content is stored or maintained by the Provider as part of the Hosted Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Hosted Services.

**4.** **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data processed by the Provider pursuant to the Hosted Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

**5.** **Subprocessors.** Provider shall enter into written agreements with all Subprocessors utilized by Provider to provide the Hosted Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

## ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 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 Hosted Services and Customer Content.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access to LEA's instance of the Hosted Services. 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 state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Authorized Use**. The Customer Content provided pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the provision of the Hosted Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Customer Content provided under the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of its software, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and

(b) Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in the Service Agreement, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in

the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request. Notwithstanding the foregoing, upon termination of the Service Agreement and the LEA's use of the Hosted Services, if LEA requires a copy of any Student Data entered into the Hosted Services, LEA shall submit the request for the data no later than twenty (20) days after termination.

a. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement.

**6. Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Hosted Services to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Hosted Services to LEA.

## ARTICLE V: DATA PROVISIONS

**1. Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to: the measures described in the Service Agreement and the Information Security Schedule attached hereto as Exhibit F.

**a. Passwords and Employee Access.** Access Control is set forth in Exhibit F.

**b. Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

**c. Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose the Service Agreement.

**d. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

**e. Security Technology.** When the Hosted Services are accessed using asupported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

**f. Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

**i. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessment of Subprocessors to determine their compliance with this Article.

**g. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

**2. Data Breach.** Data Breach is equivalent to a Security Incident as defined in Section 12 of Exhibit F and all relevant information is set forth therein. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall comply with Civil Code section 1798.82 and the procedures stated in Section 12 of its Information Security Schedule, attached hereto as Exhibit "F".

**a.** Provider agrees to adhere to all requirements in applicable State and in federal law 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.

**b.** 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 copy of said written incident response plan.

**c.** Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access.

**d.** In the event of a breach originating from LEA's use of the Hosted Services, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI- GENERAL OFFER OF PRIVACY 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or

so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Customer Content pursuant to Article V, section l (b), and Article II, section 3, above.

4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. **Designated Representatives**

The designated representative for the LEA for this Agreement is:
Name: Michelle Bennett
Title: Specialist – IT Contracts

Contact Information:
Irvine Unified School District
5050 Barranca Parkway
Irvine, CA 92602
949-936-5022
MichelleBennett@iusd.org

The designated representative for the Provider for this Agreement is:
Name: Kim Fuller-Ames
Title: Strategic Account Executive

Contact Information:
100 Washington Avenue South, Suite 1100, Minneapolis, MN 55401
(612) 716-0702
kim.ames@jamf.com

b. **Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Jeff Lendino<br>Title: General Counsel

Contact Information:
100 Washington Avenue South, Suite 1100, Minneapolis, MN 55401
(612) 605-6625
legal@jamf.com

6. **Entire Agreement.** This DPA constitutes 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, except the Service Agreement. 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.

7. **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.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF ORANGE COUNTY, CALIFORNIA, 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 ORANGE COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the DPA.

10. **Waiver.** No delay or omission of a Party to exercise any right hereunder shall be construed as a waiver of any such right and each Party reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **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.

*[Signature Page Follows]*

**IN WITNESS WHEREOF,** the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

IRVINE UNIFIED SCHOOL DISTRICT

By: ____________________ Date: March 18, 2020

Printed Name: John Fogarty Title/Positon: Asst. Supt. Business Services/CFO

IUSD Board Approval: March 17, 2020

JAMF Software, LLC

By: ____________________ Date: March 11, 2020

Printed Name: Jill Putman Title/Positon: Chief Financial Officer

***Note: Electronic signature not permitted.***

**EXHIBIT "A"**

DESCRIPTION OF SERVICES

Hosted Services as defined in the Service Agreement and Documentation.

## EXHIBIT "B"

SCHEDULE OF DATA

Data that may be processed if and when entered into the Hosted Services may include the following types of data:

Names, IP addresses, telephone number, computer names, job titles and functions and email addresses.

Categories of data subjects may include:

LEA employees and students.

## EXHIBIT "C"

DEFINITIONS

**AB 1584, Buchanan:** The statutory designation for what is now California Education Code§ 49073.1, relating to pupil records.

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

**Customer Content**: Customer Content is defined in the Service Agreement.

**Educational Records:** Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

**NIST:** Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's Hosted Services, website, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

**Provider:** For purposes of the Service Agreement, the term "Provider" means provider of software or services, including cloud-based services, for the management of Apple devices.

**Pupil Generated Content:** The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this DPA, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

**Service Agreement:** Refers to the Purchase Agreement to which this DPA supplements and modifies.

**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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

**SOPIPA:** Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

**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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is may be processed by the Provider if entered into the Hosted Services by LEA. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a LEA's use of Provider's Hosted Services.

**SDPC (The Student Data Privacy Consortium):** Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

**Student Personal Information:** "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

**Subprocessor:** For the purposes of this Agreement, 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 the Hosted Services.

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**Third Party:** The term "Third Party" means a provider of software or services, including cloud-based services, for the management of Apple devices. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of the software or services is replaced by the term "Provider."

## EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Irvine Unified School District directs INSERT PROVDER NAME HERE 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:

| | |
|---|---|
| **Extent of Disposition**<br>Disposition shall be: | ____ Complete: Disposition extends to all categories of data. |
| | |
| **Nature of Disposition**<br>Disposition shall be by: | ____ Destruction or deletion of data.<br>____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred. Provider shall destroy or delete all Customer Content. |
| | |
| **Timing of Disposition**<br>Data shall be disposed of by the following date: | ____ As soon as commercially practicable.<br>____ By (Insert Date) ________________ |

________________________________________ ____________________

Authorized Representative of LEA Date

________________________________________ ____________________

Verification of Disposition of Data
By 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 Irvine Unified School District and which is dated March 29, 2020 to any other LEA ("Subscribing LEA") who accepts this 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 other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (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.

JAMF Software, LLC

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 Term. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

By: ______________________ Date: ______________

Printed Name: ______________________ Title/Position: ______________________

**TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW:**

Name: Jeff Lendino

Title/Position: General Counsel

Email Address: legal@jamf.com

## EXHIBIT "F"

DATA SECURITY REQUIREMENTS