Privacy Policy 2024

Effective Date: August 30, 2024

Mosyle Corporation (“we” or “us”) owns and operates https://school.mosyle.com (**“Site”**), the Mosyle Manager and Mosyle OneK12 mobile applications (**“Mosyle Apps”**) on which we provide mobile device management and security services. The Site and Mosyle Apps are together the **“Services”**.

BY USING THE SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS PRIVACY POLICY.

For the purposes of this Policy, “Users” means:
“Leaders” means the individual who initially sets up the Services (each a “Primary Leader”) and others who are granted leadership privileges by the Primary Leader;
“Administrators” means the individuals who operate the technical features available through the Services;
“Teachers” means individuals who are permitted to use the classroom features in order to manage students’ mobile devices during class time;
“Staff” means individuals who are employees or contractors for the School;
“Students” means the individuals who are enrolled at a school that uses the Services for educational purposes (**“School”**).
Leaders, Administrators and other School staff are together **“Administrative Users.”**

The data controller for the information you provide or that we collect pursuant to this Privacy Policy is: Mosyle Corporation at P.O. Box 2317, Winter Park, FL 32790, USA. If you are in the EU, UK or Switzerland, please see section 9 below to learn more about our participation in the Data Privacy Framework.

1. INFORMATION WE COLLECT

We collect the following types of information:

Personal Data

“Personal Data” is any information relating to a User that identifies or can be used to identify that User, either separately or in combination with other readily available data that is received by us. As a Primary Leader, you voluntarily provide us this information when you initially establish an account on the Service. As of the effective date of this Privacy Policy, to establish an account for the School, we ask you to provide all the information necessary to complete the sign-up form available on

https://myschool.mosyle.com/signup/, including the School's name, website, address and your name, email, and phone. Once the School's account is established, you (as Primary Leader) will have the power to freely register, manually or by using integrations with a third-party software, all the other Users, providing information such as name, email and role (the **"School's Data"**).

We don't ask the School to share Personal Data of its Users as part of the School's Data. We don't request any Personal Data from any other User other than the Primary Leader. The information that is part of the School's Data is only intended to allow the School to use the Services in an efficient manner and also to internally identify which User is currently assigned to each managed device.

Also, the Services can be technically used without any School's Data, just by using only the Managed Device Information to organize and manage the devices.

We, as a Processor of the School's Data, are not responsible and have no available methods to validate if the School's Data is accurate and represents or not a natural person.

The School and the Primary Leader also represent and warrant that they will require Users to read this Privacy Policy.

Finally, when Administrative Users and Teachers log on to their accounts, we will record their geo-location, IP address and/or unique mobile device identifier and may tie it to their specific account.

We do not knowingly collect Personal Data through the sign-up form on our Site from anyone under age 16. If you are under 16, please do not leave your contact information on our Site. If you are a parent or guardian of a child under 16 years old and you learn that your child has left Personal Data on our Site, please contact us at legal@mosyle.com. Students' login credentials are based on codes generated by us based on information provided by the Administrative Users.

Except as described in this Privacy Policy, we do not request or knowingly receive Personal Data from Students or anyone else who is younger than the age of majority in their place of residence.

In addition, if a User provides us feedback or contacts us (for support, for example), we will collect the data included in the communication.

Usage Information

When an Administrative User or a Teacher uses the Services, we may automatically record certain information from them including IP address or other device address or ID, web browser and/or device type, the actions performed on the Service, and the dates and times of the access or use of the Service.

We also collect information regarding the Administrative User's interaction with email messages, such as whether they open, click on, or forward a message. This information is gathered from Administrative Users and Teachers only. We do not collect usage information or email tracking from Students.

Managed Device Information

The Services are intended to allow Schools to remotely deploy, manage, and protect supported mobile devices used by their Users. For this reason, getting information about all devices managed by our Services is one of the main reasons why a School hires our Services.

Managed Device Information consists of information about the devices and from which Mosyle is not able to identify an individual. However, based on the information of which device is assigned to each User registered by the School as part of the School's Data, Administrative Users and Teachers can possibly tie Managed Device Information to Users. The assignment of a Managed Device to a User is not required for the usage of the Services; rather, it is an option offered for Administrative Users.

For Managed Devices running iOS and iPadOS:

Device name;
Supervision mode status;
Model;
Serial number;
Wifi MAC Address;
Bluetooth status;
Bluetooth MAC Address;
Last WAN IP;
Battery level;
Total and available storage;
IMEI number;
Device UUID;
Cellular Network information;
Data/Voice Roaming status;
Personal Hotspot status;
Device Passcode status;
Last known Wi-fi SSID;
Activation Lock status;
Device Attestation;
Operating System and Build Version;

Find My iPad/iPhone status;
“Do Not Disturb” status;
Time Zone;
Accessibility Settings;
iCloud backup status. Only YES or NO. No information about which Apple ID is being used is accessed by the Services;
Last iCloud backup date and time;
iTunes Account active. Only YES or NO. No information about which Apple ID is being used is accessed by the Services;
GPS location if approved by the User or when Lost Mode is enabled;
List of apps installed and removed and the date and time we identified that. We only have access to the information of the name of the Apps installed and removed. We do not track or save any information about the usage of the apps;
List of books installed and removed on iBooks and the date and time we identified that. We only have access to the information of the name of the Books installed and removed. We do not track or save any information about the usage of the books;
List of management profiles and certificates installed on the device.

For Managed Devices running watchOS (Apple Watches): Devices running watchOS are managed in connection with the paired iOS device and information collected may include same information as the paired iOS device.

For Managed Devices running macOS (Apple computers):
Device name;
Serial number;
List of Extensions installed;
Model;
Device UUID;
Wifi MAC Address;
Ethernet MAC Address;
Battery Level and Health;
Last WAN IP;
Local hostname;
Hostname;
Operating System and Build Version;
Total and available storage;
System Integrity Protection enabled (YES or NO);
Screen Sharing Status. Only CONNECTED or DISCONNECTED;

iTunes Account active. Only YES or NO. No information about which Apple ID is being used is accessed by the Services;
Current console user nickname;
Bluetooth status;
Last known Wi-fi SSID;
Last Reboot date and time;
CPU Model;
Apple T2 Security Chip;
Activation Lock bypass status and code;
User triggered Activation Lock status;
VPN status;
IP address;
Content Caching information;
Lights out Management Details;
Security information: FileVault status; personal recovery key if escrowed; Firewall status; Firmware password status; Authenticated Root Volume Status; Bootstrap Token Status and token;
Secure Boot settings;
Installed memory;
List of apps installed and removed and the date and time we identified that.
List of background items and the status (ENABLED or DISABLED);
List of books installed and removed on iBooks and the date and time we identified that. We only have access to the information of the name of the Books installed and removed. We do not track or save any information about the usage of the books;
List of management profiles and certificates installed on the device;
Customized Device Information: Due to technical possibilities on macOS, our Services allow Administrative Users to freely create, distribute and execute on macOS devices customized scripts in order to perform tasks and get information that are not available through the standard features provided by the Services. We don't have any control of the customized scripts created, distributed and executed on macOS Managed Devices using our Services and we also have no control about any additional information not described above that Companies can collect through our Services by using customized scripts.
Screen view during the class time and if the device is connected to the same network used by the Teacher's device. For security reasons, the screen view is only enabled during the moment that device is connected to an active class by an Administrative User or a Teacher and only internally on the network. No remote screen view is supported for Users that are not on the same network.
Start and end date and time of usage of installed apps during an active class.
Please see HOW WE USE AND SHARE USAGE INFORMATION AND MANAGED DEVICE INFORMATION for more information.

DNS Data

For organizations using the Mosyle OneK12 DNS Filtering (“DNS Filtering”) for online security and compliance, information about all websites or online services accessed on Managed Devices may be collected based on the Administrator’s configurations. DNS Filtering data may contain sensitive information and should only be collected in accordance with company policies and local regulations. Administrators may choose to log a device identifier, IP address, and even log all resolved requests as needed.

Cookies

In order to personalize the Service, we use cookies, or similar technologies like single-pixel gifs and web beacons, to record log data. We use both session-based and persistent cookies. Session- based cookies last only while your browser is open and are automatically deleted when you close your browser. Persistent cookies last until you delete them or until they expire. They are unique and allow us to do analytics (as described below) and customization. You can refuse to use cookies by turning them off in your browser. You do not need to have cookies turned on to use most of the Services. You may, however, find that some areas on the Services are slower or do not function at all if cookies are disabled. To learn more about cookies generally, visit http://www.allaboutcookies.org.

Analytics

We use Google Analytics to measure and evaluate access to and traffic on the public area of the Site, and create user navigation reports for our Site administrators. Google operates independently from us and has its own privacy policy, which we strongly suggest you review. Google may use the information collected through Google Analytics to evaluate Users' and another visitor’s activity on our Site. For more information, see Google Analytics Privacy and Data Sharing.

We take measures to protect the technical information collected by our use of Google Analytics. The data collected will only be used on a need to know basis to resolve technical issues, administer the Site and identify visitor preferences; but in this case, the data will be in non- identifiable form. We do not use any of this information to identify Visitors or Users.

You may opt out from the collection of navigation information about your visit to the Site by Google Analytics by using the Google Analytics Opt-out feature.

2. HOW WE USE PERSONAL DATA

We use the Personal Data we collect as described above

To customize and analyze the Service.

To enhance your experience of Services.

To verify your eligibility for the Services.

To contact you regarding your account.

To prevent, detect and fight fraud or other illegal or unauthorized activities.

Address ongoing or alleged fraud on or though the Services and our related products and services;
Analyze data to better understand and design countermeasures against fraud;
Retain data related to fraudulent activities to prevent recurrence.

To ensure legal compliance.

Comply with legal requirements;
Assist law enforcement;
Enforce or exercise our rights.

To process your information as described in this Privacy Policy, we rely on the following legal bases:
Legitimate interests: We may use your information where we have legitimate interests to do so. For example, we analyze our users' behavior to improve the Services, to prevent and detect fraud and misuse, and to market new products and services that we think will interest you;
Consent: From time to time, we may ask for your consent to use your information. You may withdraw your consent at any time by contacting us at legal@mosyle.com.
You may stop receiving promotional emails from us by clicking the unsubscribe link at the bottom of the promotional email. Communication related to important changes on Services are not considered promotional email.

3. HOW WE SHARE PERSONAL DATA

We will not sell, rent, or share Personal Data or School's Data with third parties except in the following ways:

We use third-party operational providers to help us operate and improve the Services. These third parties assist us with data hosting and maintenance, analytics, customer care, marketing, payment processing, debt collection and security operations. All of our service providers must adhere to confidentiality obligations that are consistent with this Privacy Policy.
Applicable law may require us and our service providers to disclose your information if: (i) reasonably necessary to comply with a legal process, such as a court order, subpoena or search warrant, government investigation or other legal requirements; or (ii) necessary for the prevention or detection of crime (subject in each case to applicable law).
We may also share information: (i) if disclosure would mitigate our liability in an actual or threatened lawsuit; (ii) as necessary to protect our legal rights and legal rights of our users, business partners or other interested parties; (iii) to enforce our agreements with you; and (iv) to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing.
We may transfer your information if we are involved, whether in whole or in part, in a merger, sale, acquisition, divestiture, restructuring, reorganization, dissolution, bankruptcy or other change of

ownership or control.
We may ask for your consent to share your information with third parties. When we do, we will make clear why we want to share the information.

4. HOW WE USE AND SHARE USAGE INFORMATION AND MANAGED DEVICE INFORMATION

We use the Usage Information and Managed Device Information for the following purposes: (i) to monitor the effectiveness of our Service; (ii) to monitor aggregate metrics such as use and demographic patterns; and (iii) to diagnose or fix technology problems reported by our Users or our employees; (iv) to provide usage trends reports ("Trends") to support recommendation and statistics to our Users. In those cases, the information will be de-identified, and will only be based on general information combined through our algorithms with Usage Information and Managed Device Information.

Also, you authorize us to use, in aggregated form, the de-identified Usage Information and Managed Device Information to: (i) create, publish and sell any kind of public or private reports and other informational content; (ii) to assist such parties in understanding our Users' interests, habits, and usage patterns for certain programs, content, services, advertisements, promotions, and/or functionality available through the Services; or (iii) for any other business or marketing purposes decided by us.

5. HOW WE PROTECT YOUR INFORMATION

We take the security of your Personal Data and School's Data seriously and use appropriate technical, administrative, and physical measures designed to protect your Personal Data against unauthorized or unlawful processing and against accidental loss, destruction or damage. This includes, for example, encryption, firewalls, password protection and other access and authentication controls. We also limit access to Personal Data and School's Data to employees who reasonably need access to it to provide products or services to you, or in order to do their jobs. However, because no security system can be 100% effective, we cannot completely guarantee the security of any information we may have collected from or about you.

6. HOW LONG WE RETAIN PERSONAL DATA

We retain Personal Data and School's Data based on the following criteria:
a) Active School's Data: School's Data, including devices under management, users and other data currently in use and not deleted on your account. Active School's Data is retained for as long as your account is active or until it's manually removed from your account by an Administrator.
b) Active School's Data Backups: Mosyle performs full daily Backups for all Active School's Data and stores such backups in a Recovery Datacenter for up to 15 days. After 15 days, the Backup is deleted.

Based on this flow, any information manually removed from your account by an Administrator will still be retained as part of the Active School's Data Backup for up to 15 days.
c) Administrative Users Logs: Mosyle logs relevant actions performed by Administrative Users when operating the features offered by the Services. Administrative Users Logs can be retained for up to 60 days from the day the logged action occurred. After 60 days the Administrator Log will be automatically deleted from production environment. Administrator Logs are part of the Active School's Data Backups described in section 6 "b" above and after the deletion from the production environment, Administrator Logs may be part of the Active School's Data Backups for up to 15 days.
d) Support Logs: When you create a support ticket, depending on the complexity of the question or request, it may be necessary for engineers on Mosyle's Technical Support team to prepare and implement special logs that will be used to support you. Those logs may include School's Data. Support Logs will be retained for up to 15 days. Logs are part of the Acive Company's Data Backups described in secion 6 "b" above and ajer the deleion from the producion environment, Administrator Logs may be part of the Acive Company's Data Backups for up to 15 days.
e) Support Ticket Attachments: When you create a support ticket, our Services give you the option to attach files to the ticket. Mosyle doesn't expect to receive any sensitive or protected information from Support Ticket Attachments, including any School's Data. If you need to submit any proprietary information as an attachment of a Support Ticket, please share that with our Support Team before any submission so you can receive correct instructions. Support Ticket Attachments may be retained for up to 30 days and will not be part of any backup.

As an exception, we may retain Personal and School's Data for periods that are longer than the periods described on this Section 6 based on the following reasons:
Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them);
Whether retention is advisable considering our legal position (such as, for statutes of limitations, litigation or regulatory investigations).

7. YOUR CHOICES ABOUT YOUR INFORMATION

We respect your privacy rights and provide you with reasonable access to the Personal Data that you may have provided through your use of the Services. If you wish to access or amend any other Personal Data we hold about you, you may contact us by opening a new support ticket or emailing us at legal@mosyle.com. At your request, we will have any reference to you deleted or blocked in our database.

As a Primary Leader, if you want to delete the Personal Data you provided to us in order to have an account with us for the School you represent, we will need to receive from you the necessary information to set another person with the School you represent to act as the Primary Leader. By doing that, you

represent and warrant that you obtained the necessary approvals from this person and required them to read our Privacy Policy.

You, as a Primary Leader, may update, correct, or delete your Account information and preferences at any time by opening a new support ticket.

Please note that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, we may retain all information you submit for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so.

You may decline to provide Personal Data, in which case we will not be able to establish an account to the School you represent or provide our Services to your School.

At any time, you may object to the processing of your Personal Data, on legitimate grounds, except if otherwise permitted by applicable law. If you believe your right to privacy granted by applicable data protection laws has been infringed upon, please contact us at legal@mosyle.com.

You also have a right to lodge a complaint with data protection authorities.

This provision does not apply to potential Personal Data that is part of School's Data. In this case, the management of the School's Data is subject to the School's own Privacy Policy, and any request for access, correction or deletion should be made to the School responsible for the uploading and storage of such data into our Service.

Based on the permissions granted by the Primary Leader, Administrative Users can at any time update, correct, or delete any information, including potential Personal Data, that is part of the School's Data registered, uploaded and stored into our Service.

We have no direct relationship with the Users created by the School by the upload and storage of the School's Data, whose potential Personal Data it may process on behalf of a School. An individual who seeks access, or who seeks to correct, amend, delete inaccurate data should direct his or her query to the School or Administrative User they deal with directly.

If the School requests us to remove the data, we will respond to its request within thirty (30) days. We will delete, amend or block access to any Personal Data and School's Data that we are storing only if we receive a written request to do so from the Primary Leader who is responsible for such Account, unless we have a legal right to retain such Personal Data or School's Data. We reserve the right to retain a copy of such data for archiving purposes, or to defend our rights in litigation.

8. CROSS-BORDER DATA TRANSFERS

Sharing of information sometimes involves cross-border data transfers to or from the United States of America and other jurisdictions. For example, when the Services are available to users in the European Economic Area ("EEA"), Personal Data is transferred to the United States. We use the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) and standard contractual clauses approved by the European Commission to validate transfers of EEA residents' personal information from the EEA to other countries. Standard contractual clauses are commitments between companies transferring personal information of EEA residents to protect the privacy and security of the transferred personal information. Please see Section 9 for information about our participation in the EU-US and Swiss-US EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

9. OUR PARTICIPATION IN THE DATA PRIVACY FRAMEWORK

Mosyle complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Mosyle has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Mosyle has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/. With respect to EU, UK, or Swiss Personal Data received or transferred pursuant to the Data Privacy Frameworks, Mosyle is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

Definitions. In this section, the following terms have the following meanings:

"EU Personal Data" means any information relating to a EU User that identifies or can be used to identify that EU User, either separately or in combination with other readily available data that is received by Mosyle in the U.S. from the EEA, UK, or Switzerland in connection with the Services, including information provided offline, including Sensitive Personal Data.

"Sensitive Personal Data" means EU Personal Data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data

that uniquely identifies an individual, physical or mental health, or sexual life or orientation.
"EU User" means a User who resides in the EEA, UK or Switzerland.

Data Privacy Framework Principles. Mosyle commits to processing EU Personal Data in accordance with the DPF Principles as follows:

(1) Notice
Prior to collecting EU Personal Data, Mosyle notifies EU Users about the categories of EU Personal Data that Mosyle collects and the purposes for collection and use of their EU Personal Data. Mosyle will only process EU Personal Data in ways that are compatible with the purpose for which Mosyle collected it or for purposes later authorized.

We use the EU Personal Data that we collect from EU Users of the Services as described in this Privacy Policy. Before Mosyle uses EU Personal Data for a purpose that is materially different from the purpose for which Mosyle collected it or that was later authorized, Mosyle will provide EU Users with the opportunity to opt out.

(2) Choice
If Mosyle collects Sensitive Personal Data, we will obtain explicit opt-in consent whenever the DPF requires. Mosyle will obtain opt-in consent before EU Personal Data is disclosed to third parties other than those described in this Privacy Policy, before EU Personal Data is used for a different purpose than that purpose for which it was collected or later authorized, and whenever the DPF requires.

Please see the **YOUR CHOICES ABOUT YOUR INFORMATION** section above for more information about how to exercise your choices.

(3) Accountability for Onward Transfer
Mosyle shares EU Personal Data collected through the Services as described above.
If Mosyle transfers Personal Data to a third party, Mosyle takes reasonable and appropriate steps to ensure that each third party transferee processes Personal Data transferred in a manner consistent with Mosyle's obligations under the DPF Principles. Mosyle will ensure that each transfer is consistent with any notice provided to EU Users and any consent they have given. Mosyle requires a written contract with any third party receiving EU Personal Data that ensures that the third party (i) processes the Personal Data for limited and specified purposes consistent with any consent provided by EU Users, (ii) provides at least the same level of protection as is required by the DPF Principles, (iii) notifies Mosyle if it cannot comply with the DPF; and (iv) ceases processing EU Personal Data or takes other reasonable and

appropriate steps to remediate.

As noted above, under certain circumstances, Mosyle may be required to disclose EU Personal Data in response to valid requests by public authorities, including for national security or law enforcement requirements.

Mosyle remains liable under the DPF Principles if an agent processes EU Personal Data in a manner inconsistent with the Principles unless Mosyle is not responsible for the event giving rise to the damage.

(4) Security
Mosyle takes appropriate measures to protect EU Personal Data from loss, misuse and unauthorized access, disclosure, alteration, unavailability and destruction. In determining these measures, Mosyle takes into account the risks involved in the processing and the nature of the EU Personal Data.

(5) Data Integrity and Purpose Limitation
Mosyle takes reasonable steps to ensure that such EU Personal Data is reliable for its intended use, accurate, complete and current. Mosyle adheres to the DPF Principles for as long as it retains EU Personal Data in identifiable form. Mosyle takes reasonable and appropriate measures to comply with the requirement under the DPF to retain EU Personal Data in identifiable form only for as long as it serves a purpose of processing.

Mosyle limits the collection of EU Personal Data to information that is relevant for processing. Mosyle does not process EU Personal Data in a way that is incompatible with the purpose for which it was collected or subsequently authorized by an EU User.

(6) Access
An EU User has the right to access their EU Personal Data and to correct, amend, limit use of or delete the EU Personal Data if the Personal Data is inaccurate or processed in violation of the DPF Principles. Mosyle is not required to grant the rights to access, correct, amend and delete EU Personal Data if the burden or expense of providing access, correction, amendment or deletion is disproportionate to the risks to the EU User's privacy or if the rights of persons other than the EU User are or could be violated.

Please see the **YOUR CHOICES ABOUT YOUR INFORMATION** section above for more information about how to exercise your choices.

(7) Recourse, Enforcement, and Liability
In compliance with the DPF Principles, Mosyle commits to resolve complaints about your privacy and our collection or use of your Personal Data transferred to the United States pursuant to DPF. European Union,

UK, and Swiss individuals with Data Privacy Framework inquiries or complaints should first contact Mosyle at legal@mosyle.com.

In compliance with the EU-U.S. DPF and the UK Extension to the EU- U.S. DPF and the Swiss-U.S. DPF, Mosyle commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF. If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Data Privacy Framework Annex 1 at https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction.
Mosyle commits to periodically review and verify its compliance with the Data Privacy Framework Principles and to remedy any issues arising out of failure to comply with the DPF Principles. Mosyle acknowledges that its failure to provide an annual self-certification to the U.S. Department of Commerce will remove it from the Department's list of Data Privacy Framework participants.

10. YOUR CALIFORNIA PRIVACY RIGHTS

If you are a California resident, you can request a notice disclosing the categories of Personal Data about you that we have shared with third parties for their direct marketing purposes during the preceding calendar year. At this time, Mosyle does not share Personal Data with third parties for their direct marketing purposes.

11. CHILDREN UNDER 16

The Services are not intended to be managed by individuals under the age 16. If we become aware that person managing our Services and submitting information is under age 16, we will delete the information as soon as possible. Except as described in this Privacy Policy, we do not request or knowingly receive Personal Data from Students or anyone else who is younger than the age of majority in their place of residence.

12. CHANGES TO THIS PRIVACY POLICY

The Effective Date at the top of this page indicates when this Privacy Policy was last revised. Unless applicable law prevents or a change is needed to protect the privacy or security of our users, we will notify you at least fifteen (15) days before any material change takes effect so that you have time to review the changes before they are effective. The previous version of this Privacy Policy will apply until

the Effective Date. Your use of the Services after the Effective Date means that you accept the Privacy Policy as revised.

13. QUESTIONS

If you ever have questions about our online Privacy Policy, please contact us via email at legal@mosyle.com.