

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and _____ ("Service Provider") on _____ ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.
Agree: Yes No

5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
Agree: Yes No N/A

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
Agree: Yes No

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
Agree: Yes No

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
Agree: Yes No N/A

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.
Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No

5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No **We do not target advertise to students**

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No **We do not target advertise to students**

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Kathy A. Robinson
Print Name

Kathy A. Robinson 3/4/24
Signature, Date
VPA Sales & Acct Mgt.
ATR

Laura Assem
Print Name (Roseville City School District)

Laura Assem 3/15/2024
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Section 1.7: Internal Security

Section II.2: Exporting of Student-Created Content

Section II.4: Review and Correcting Personally Identifiable Information (PII)

EXHIBITS

Section II.5: Securing Student Data

Section II.6: Disclosure Notification

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Section III.5: How Student Data is Protected:

Section 1.6 External Security

We use the Cisco Meraki software for our network which includes the Firewall and IDS built into it, and we are on the latest version of Meraki. The majority of our system is internal and only accessible at the physical building and network so most of our external contact comes from our Sales representatives reaching out to schools, who are trained in common social engineering attacks like phishing attacks. Our emails go through Microsoft Exchange and are filtered according to Microsoft's security standards. Any suspicious emails are automatically blocked and quarantined by Microsoft Defender and can be reviewed by our IT team. If any emails do get through this filtering process, our sales reps are always on the lookout for suspicious emails. Each computer is protected by Webroot Business Endpoint Protection and Microsoft Defender, and in the event that one of our sales reps gets attacked, our IT department is always ready to remotely connect to the affected computer using our Remote Desktop Access solution. Lastly, any systems that are not on-premise, are located in the Microsoft Azure Cloud and adhere to the security standards of Azure.

Section 1.7: Internal Security

The initial process consists of a data entry step where our Data Entry team cleans and enters the data into our system. Once in our system, we store the class list provided by the school in the cloud where it's rarely accessed again. The data from the district/school is then handled by our Print team to fulfill the initial custom order forms with the children's art and name. Lastly, the order forms go through our production and shipping teams to pack and ship the order forms to the school. When an order comes in from a parent, we use the student, teacher, and school names on our stickers and substrate to help facilitate the production, packing, and shipping of the order. Any additional data is only made accessible to managers through role-based access controls and enforced by Active Directory groups.

Once the data is uploaded to our system, it is kept secure in the Microsoft Azure cloud and only made accessible to our applications through our API. Our data is backed up using Azure's backup process which takes multiple snapshots throughout the day and has a retention of 35 days. All backups are encrypted using AES 256-bit encryption and cannot be exported from Azure. After the 35-day retention period, all backup snapshots are permanently deleted automatically by Azure. The only personnel that have access to this data directly are our Azure Administrators.

Lastly, any hard copies printed by our personnel are disposed of securely using a third-party company called QuickShred. They provide us with locked containers throughout our facility that cannot be opened. These containers are picked up when full and documents are professionally disposed of.

Section II.2: Exporting of Student – Created Content

We scan the children's artwork and create an online code that the parent can use on our website to access their child's artwork. Each code is unique to that child's artwork. There is also a QR code that will direct them to their child's artwork.

Section II.4: Reviewing and Correcting Personal Identifiable Information

Accessing and Correcting Your Information

You can review and change your personal information by logging into the Website and visiting your account profile page.

You may also send us an email at info@arttoremember.com to request access to, correct or delete any personal information that you have provided to us. We may not be able to delete your personal information except by also deleting your user account. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

We reserve the right to send you communications relating to the services we provide, such as service announcements and administrative messages, which are considered part of your account membership. You cannot opt-out from receiving those messages, but you may terminate your account at any time.

If you delete your User Contributions from the Website, copies of your User Contributions may remain viewable in cached and archived pages or might have been copied or stored by other Website users. Proper access and use of information provided on the Website, including User Contributions, is governed by our Terms of Use.

Section II.5: Securing Student Data

The initial process consists of a data entry step where our Data Entry team cleans and enters the data into our system. Once in our system, we store the class list provided by the school in the cloud where it's rarely accessed again. The data from the district/school is then handled by our Print team to fulfill the initial custom order forms with the children's art and name. Lastly, the order forms go through our production and shipping teams to pack and ship the order forms to the school. When an order comes in from a parent, we use the student, teacher, and school names on our stickers and substrate to help facilitate the production, packing, and shipping of the order. Any additional data is only made accessible to managers through role-based access controls and enforced by Active Directory groups.

Once the data is uploaded to our system, it is kept secure in the Microsoft Azure cloud and only made accessible to our applications through our API. Our data is backed up using Azure's backup process which takes multiple snapshots throughout the day and has a retention of 35 days. All backups are encrypted using AES 256-bit encryption and cannot be exported from Azure. After the 35-day retention period, all backup snapshots are permanently deleted automatically by Azure. The only personnel that have access to this data directly are our Azure Administrators.

Lastly, any hard copies printed by our personnel are disposed of securely using a third-party company called QuickShred. They provide us with locked containers throughout our facility that cannot be opened. These containers are picked up when full and documents are professionally disposed of.

Section II.6: Disclosure Notification

We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure. The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Website, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our Website. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Website.

Section II.8: Family Educational Rights and Privacy Act Compliance

A2R, Inc. d/b/a Art to Remember Website Privacy Policy

Last modified: February 2023

Introduction

A2R, Inc. d/b/a Art to Remember, an Indiana corporation (“Company,” “we,” “our,” or “us”), respects your privacy and is committed to protecting it through our compliance with this policy. This policy describes the types of information we may collect from you or that you may provide when you visit the website www.arttoremember.com (“Website”) and our practices for collecting, using, maintaining, protecting, and disclosing that information. Terms not defined herein have the same meaning as in the Website Terms of Use (“Terms of Use”), and this policy is subject to the Terms of Use.

The Company’s mission is to preserve memories and support art education and our art-based school fundraising programs are the primary manner in which we pursue our mission. In order to efficiently and effectively run our programs and raise funding for art education, we collect certain information from participating schools, Parents, Artists, and other users of the Website.

This policy applies to information we collect:

On this Website.

In email, text, and other electronic messages between you and this Website.

Through mobile and desktop applications you download from this Website, which provide dedicated non-browser-based interaction between you and this Website.

It does not apply to information collected by:

Us offline or through any other means, including on any other website operated by Company or any third party; or

Any third party, including through any application or content that may link to or be accessible from or on the Website.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use our Website. By accessing or using this Website, you agree to this privacy policy. This policy may change from time to time. Your continued use of this Website after we make changes is deemed to be acceptance of those changes.

The Website may contain links to other websites. This privacy policy only applies to the Website. We cannot and do not control and are not responsible for the practices of other parties or the content of other websites which are linked to or integrated with the Website. You should check the privacy policies of any third-party website before providing your personal information to them.

Children Under the Age of 18

Our Website is not intended for children under 18 years of age. No one under age 18 may provide any information to or on the Website. We do not knowingly collect personal information from children under 18. If you are under 18, do not use or provide any information on this Website or through any of its features, register on the Website, make any purchases through the Website, use any of the interactive or public comment features of this Website, or provide any information about yourself to us, including your name, address, telephone number, email address, or any screen name or user name you may use. If we learn we have collected or received personal information from a child under 18 without verification of parental consent, we will delete that information.

California residents under 16 years of age may have additional rights regarding the collection and sale of their personal information. Please see Your State Privacy Rights for more information.

Information We Collect About You and How We Collect It

We collect several types of information from and about users of our Website, which may include:

Personal Information. Information by which you may be personally identified, such as name, postal address, email address, telephone number, and/or any other identifier by which you may be contacted online or offline (“personal information”);

Non-Identifying Information. Information that is about you but individually does not identify you;

Class Lists. We collect a “Class List” from each school participating in a Company fundraiser. Class Lists are submitted by School Coordinators and may include the name and homeroom teacher of each participating Artist. For schools that have policies prohibiting providing full names, School Coordinators may submit a modified Class List which only provides an Artist’s first name and last initial, last name and first initial, or unique codes for each Artist. School Coordinators are encouraged to provide at least first names because it enhances the experience for the Artists and their families and drives better fundraising results for the school;

Artwork. The Company also uses the Class Lists to generate labels for each participating Artist. These labels are sent to the applicable school for their use in submitting Artists’ artwork. These

labels are placed on the back of each Artist's artwork delivered to the Company to identify the Artist for each artwork;

Orders and Online Ordering. The Company also uses the Class Lists and artwork to create personalized order forms and online order codes for each Artist. Personalized order forms (which include unique online order codes for each Artist) are delivered to schools and distributed by the schools to the Artists for ordering purposes. Parents or other authorized users complete an order by providing the information requested which includes personal information such as name, email address, phone number, ship to address, billing name and address, and credit card number and expiration date;

Artist's Information. The Company cannot control what information is submitted by School Coordinators or Parents. Except as set forth above, we will not knowingly collect personal information about children without obtaining parental consent;

Information Under School's Control. Once these labels, order forms, or online order codes are in a school's or Parent's possession, the Company cannot control further distribution or disclosure of such information and it is the school's and/or Parent's sole responsibility to maintain the privacy of any such information; and/or

Internet, Equipment and Usage. Information about your internet connection, the equipment you use to access our Website, and usage details.

We collect this information:

Directly from you when you provide it to us.

Automatically as you navigate through the Website. Information collected automatically may include usage details, IP addresses, and information collected through cookies, web beacons, and other tracking technologies.

Information You Provide to Us

We only work with schools and organizations which have agreed to work with us to promote and support their art education programs and Parents that create their own account and upload artwork and other materials to their account. School Coordinators and Parents voluntarily submit the artwork of their Artists to us. The Company claims no copyright in any artwork submitted to us and will not use artwork for any purpose other than running its school fundraising programs or fulfilling an order or otherwise complying with a Parent request without the written permission of an Artist's Parent.

The information we collect on or through our Website may include:

Information that you provide to the Website. This includes information provided at the time of registering to use our Website, purchasing products and/or services, subscribing to our services, posting or uploading artwork or other material, or requesting further services. We may also ask you for information when you enter a contest or promotion sponsored by us, and when you report a problem with our Website.

Records and copies of your correspondence (including email addresses), if you contact us.

Your responses to surveys that we might ask you to complete for research purposes.

Details of transactions you carry out through our Website and of the fulfillment of your orders. You may be required to provide financial information before placing an order through our Website.

You also may provide information to be published or displayed (hereinafter, “posted”) on public areas of the Website, or transmitted to other users of the Website or third parties (collectively, “User Contributions”), such as through bulletin boards, blogs, or other public discussion forums on the Website. Your User Contributions are posted on and transmitted to others at your own risk; no security measures are perfect or impenetrable. Additionally, we cannot control the actions of other users of the Website with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed by unauthorized persons. A user of the Website may voluntarily choose to submit personally identifiable data to such forums. Any personal information you choose to submit in such a forum may be read, collected, or used by others who visit these forums, and may be used to send you unsolicited messages or for other purposes outside of the Company’s control. We are not responsible for the personal information you choose to submit in these forums.

Information We Collect Through Automatic Data Collection Technologies

As you navigate through and interact with our Website, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including:

Details of your visits to our Website, including traffic data, location data, and other communication data and the resources that you access and use on the Website.

Information about your computer and internet connection, including your IP address, operating system, and browser type.

We also may use these technologies to collect information about your online activities over time and across different websites or other online services (behavioral tracking).

The information we collect automatically is only statistical data and does not include personal information. It helps us to improve our Website and to deliver a better and more personalized service, including by enabling us to:

Estimate our audience size and usage patterns.

Store information about your preferences, allowing us to customize our Website according to your individual interests.

Speed up your searches.

Recognize you when you return to our Website.

The technologies we use for this automatic data collection may include:

Cookies (or browser cookies). A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of our Website. Unless

you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our Website.

Flash Cookies. Certain features of our Website may use local stored objects (or Flash cookies) to collect and store information about your preferences and navigation to, from, and on our Website. Flash cookies are not managed by the same browser settings used for browser cookies.

Web Beacons. Pages of our the Website may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity).

Third-Party Use of Cookies and Other Tracking Technologies

We may work with third parties to monitor certain pages of the Website for the purpose of reporting website traffic, navigational, and other lawful data and statistics. Where authorized by us, these third parties may use cookies and/or other tracking technologies to compile anonymous statistics about our Website visitors. We do not control these third parties' tracking technologies.

How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal information:

To create personalized order forms, online order codes, and pages on our online ordering website.

To enhance the content with which you interact, fulfill orders, contact you, and improve the Company's fundraising programs and customer service.

For internal business purposes in accordance with the Company's mission.

To present our Website and its contents to you.

To provide you with information, products, or services that you request from us.

To fulfill any other purpose for which you provide it.

To provide you with notices about your account.

To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.

To notify you about changes to our Website or any products or services we offer or provide through it.

In any other way we may describe when you provide the information.

For any other purpose with your consent.

Disclosure of Your Information

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may disclose personal information that we collect or you provide as described in this privacy policy:

To our subsidiaries and affiliates.

To contractors, service providers, and other third parties we use to support our business and who are bound by contractual obligations to keep personal information confidential and use it only for the purposes for which we disclose it to them.

To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by the Company about our Website users is among the assets transferred.

To fulfill the purpose for which you provide it.

For any other purpose disclosed by us when you provide the information.

With your consent.

We may also disclose your personal information:

To comply with any court order, law, or legal process, including to respond to any government or regulatory request.

To enforce or apply our Terms of Use and other agreements, including for billing and collection purposes.

If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of the Company, our customers, or others.

Choices About How We Use and Disclose Your Information

We strive to provide you with choices regarding the personal information you provide to us. We have created mechanisms to provide you with the following control over your information:

Tracking Technologies. You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. To learn how you can manage your Flash cookie settings, visit the Flash player settings page on Adobe's website. If you disable or refuse cookies, please note that some parts of this Website may then be inaccessible or not function properly.

Promotional Offers from the Company. If you do not wish to have your email address used by the Company to promote our own products or services, you can opt-out by logging into the Website and adjusting your user preferences in your account profile, by checking or unchecking the relevant boxes or by sending us an email stating your request to info@arttoremember.com. If we have sent you a promotional email, you may send us a return email asking to be omitted from future email distributions. This opt out does not apply to information provided to the Company as a result of a product purchase, warranty registration, product service experience or other transactions.

Accessing and Correcting Your Information

You can review and change your personal information by logging into the Website and visiting your account profile page.

You may also send us an email at info@arttoremember.com to request access to, correct or delete any personal information that you have provided to us. We may not be able to delete your personal information except by also deleting your user account. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

We reserve the right to send you communications relating to the services we provide, such as service announcements and administrative messages, which are considered part of your account membership. You cannot opt-out from receiving those messages, but you may terminate your account at any time.

If you delete your User Contributions from the Website, copies of your User Contributions may remain viewable in cached and archived pages or might have been copied or stored by other Website users. Proper access and use of information provided on the Website, including User Contributions, is governed by our Terms of Use.

Your State Privacy Rights

State consumer privacy laws may provide their residents with additional rights regarding our use of their personal information. To learn more about California residents' privacy rights, visit our CCPA Policy. California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to info@arttoremember.com.

Colorado, Connecticut, Virginia, and Utah each provide their state residents with rights to:

Confirm whether we process their personal information.

Access and delete certain personal information.

Data portability.

Opt-out of personal data processing for targeted advertising and sales.

Colorado, Connecticut, and Virginia also provide their state residents with rights to:

Correct inaccuracies in their personal information, taking into account the information's nature processing purpose.

Opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects.

To exercise any of these rights, please send an email to info@arttoremember.com. To appeal a decision regarding a consumer rights request, please send an email to info@arttoremember.com. When contacting us regarding an exercise of rights or an appeal, please include your name, mailing address, email address, and phone number.

Nevada provides its residents with a limited right to opt-out of certain personal information sales. Residents who wish to exercise this sale opt-out rights may submit a request to this designated address: info@arttoremember.com. However, please know we do not currently sell data triggering that statute's opt-out requirements.

Data Security

We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure. The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Website, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our Website. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Website.

Changes to Our Privacy Policy

It is our policy to post any changes we make to our privacy policy on this page. If we make material changes to how we treat our users' personal information, we will notify you by email to the email address specified in your account and/or through a notice on the Website home page. The date the privacy policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable email address for you, and for periodically visiting our Website and this privacy policy to check for any changes.

Contact Information

To ask questions or comment about this privacy policy and our privacy practices or to register a complaint or concern, contact us at:

info@arttoremember.com. When contacting us pursuant to this privacy policy, please include your name, mailing address, email address, and phone number.

Section III.5: How Student Data is Protected

Information You Provide to Us

We only work with schools and organizations which have agreed to work with us to promote and support their art education programs and Parents that create their own account and upload artwork and other materials to their account. School Coordinators and Parents voluntarily submit the artwork of their Artists to us. The Company claims no copyright in any artwork submitted to us and will not use artwork for any purpose other than running its school fundraising programs or fulfilling an order or otherwise complying with a Parent request without the written permission of an Artist's Parent.

The information we collect on or through our Website may include:

Information that you provide to the Website. This includes information provided at the time of registering to use our Website, purchasing products and/or services, subscribing to our services, posting or uploading artwork or other material, or requesting further services. We may also ask you for information when you enter a contest or promotion sponsored by us, and when you report a problem with our Website.

Records and copies of your correspondence (including email addresses), if you contact us.

Your responses to surveys that we might ask you to complete for research purposes.

Details of transactions you carry out through our Website and of the fulfillment of your orders. You may be required to provide financial information before placing an order through our Website.

You also may provide information to be published or displayed (hereinafter, "posted") on public areas of the Website, or transmitted to other users of the Website or third parties (collectively, "User Contributions"), such as through bulletin boards, blogs, or other public discussion forums on the Website. Your User Contributions are posted on and transmitted to others at your own risk; no security measures are perfect or impenetrable. Additionally, we cannot control the actions of other users of the Website with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed by unauthorized persons. A user of the Website may voluntarily choose to submit personally identifiable data to such forums. Any personal information you choose to submit in such a forum may be read, collected, or used by others who visit these forums, and may be used to send you unsolicited messages or for other purposes outside of the Company's control. We are not responsible for the personal information you choose to submit in these forums.