Data Protection Policy

Museum of Chinese in America

Last updated: September 23, 2019

I. DEFINITIONS

A. **MOCA** means Museum of Chinese in America, a registered non-profit organization.

B. **Personal Information** means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

C. **Private Information** means either (i) personal information consisting of any information in combination with any one or more of the following unencrypted or otherwise unprotected data elements: (1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

D. **Register of Systems** means a register of all systems or contexts in which personal information is processed by MOCA.

E. **GDPR** means the EU General Data Protection Regulation. Where “personal information” is used in this Policy, it is intended to be used interchangeably with “personal data” under the GDPR.

F. **Breach of the Security System** means unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of private information by an employee or agent of the business for the purposes of
the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

G. Chief Technology Officer means the most senior officer who makes decisions regarding the development and application of new technologies.

H. President means the most senior executive officer responsible for implementing existing plans and policies, ensuring the successful management of the business and setting future strategy.

I. Third Party Enterprise Platform Provider means Tessitura Network, Inc. which provides a Remote Access Managed Plan that hosts and administers Tessitura software on a remote server infrastructure in its Operation Center.

II. DATA PROTECTION PRINCIPLES

A. The guiding principles of MOCA’s Data Protection Policy are transparency, security, and accountability.

1. MOCA will only collect individuals’ private information for legitimate purposes and business needs and will let consumers know what private information MOCA holds and how it uses that private information.

2. Consumers will have the right to control their private information and MOCA will take reasonable steps to keep the private information secure.

3. If a breach were to occur, MOCA will take all reasonable steps to respond to security incidents, including providing notice to affected persons and to required regulators, if necessary.

B. The purpose of this Data Protection Policy is to create a privacy program that achieves the following goals:

1. Demonstrate compliance with applicable laws and regulations.

2. Promotes consumer trust and confidence.

3. Enhance MOCA’s reputation.

4. Facilitate privacy program awareness by employees, customers, partners and service providers.

5. Respond effectively to privacy breaches.

6. Continuously maintain and improve the privacy program.
C. Specifically, MOCA is committed to processing data in accordance with applicable laws and regulations including the New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD ACT) and GDPR when applicable.¹

1. Article 39-F of New York General Business Law, Section 899-BB requires small businesses² to implement a data security program that contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business’s activities, and the sensitivity of the personal information the small business collects from or about consumers.

III. GENERAL RESPONSIBILITIES

A. All MOCA Staff

Everyone who works for MOCA has responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles individuals’ private information must ensure that it is handled and processed in accordance with this policy and data protection principles set forth herein.

1. Data Guidelines

a. MOCA will only collect individuals’ private information for legitimate purposes and business needs. Where a legitimate business need for private information exists, MOCA will retain that private information only for as long as necessary.

b. Customer credit card information should not be kept unless there exists a business need for it. Staff should not retain the account number and expiration date unless an essential business need exists to do so.

c. The only people able to access personal information covered by this policy should be those who need it for their work.

¹ To the extent that MOCA collects personal information of individuals in the European Union, MOCA will comply with the requirements of GDPR as set out in Appendix A. This policy does not expressly incorporate the requirements of the California Consumer Protection Act of 2018 (CCPA) because the CCPA does not currently apply to non-profit organizations.

² “Small Business” is defined as “any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.” See Section 899-BB 1. (c). The Shield Act does not contain any exemption for non-profit organizations.
d. Personal information **should not be shared informally**. When access to individuals’ private information is required, staff can request it from their managers.

e. All staff **should attend training** provided by MOCA designed to help staff to understand their responsibilities when handling data.

f. Staff should keep all data secure by taking reasonable precautions and following the guidelines below.

g. In particular, **strong passwords must be used** and they should never be shared.

h. Individuals’ private information **should not be disclosed** to unauthorized people, either within MOCA or externally.

i. Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

j. Staff **should request help** from their manager or the chief technology officer if they are unsure about any aspect of data protection.

2. **Data Storage**

These rules describe how and where data should be safely stored. Questions about storing data can be directed to the chief technology officer.

a. MOCA shall implement appropriate access controls for its administrative office. Staff should know what to do and whom to call if they see an unfamiliar person in MOCA’s administrative office.

b. If MOCA ships sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Overnight shipping services that allow for delivery tracking are preferred.

c. When personal information is **stored on paper/hard copy**, such paper or hard copies should be kept in a secure place where unauthorized people cannot access it according to the guidelines below:

- When not in use, paper or hard-copy files containing personal information should be kept in a **locked drawer or filing cabinet**. Access should be limited to staff with a legitimate business need.
• Staff should make sure paper and hard-copy printouts containing personal information are **not left where unauthorized people could see them**, like on a printer or on a shared desk.

• Data printouts containing personal information should be **shredded** and disposed of securely when there is no longer a legitimate business need.

• Staff must put files containing persona information away, log off their computers and lock their file cabinets and office doors at the end of the day.

d. When personal information is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts by following these guidelines:

e. Data containing personal information should be **protected by strong passwords** that are changed regularly and never shared between employees. Strong passwords are typically long and contain a mix of letters, numbers, and characters. Passwords are required to be changed when appropriate – for example, following a data breach.

f. Staff should be aware that they should not give out their passwords over the telephone to anyone, including persons purporting to be IT staff. Calls such as these are almost always fraudulent; no one should be asking staff to reveal their passwords.

g. If data containing personal information is **stored on removable media** (like a USB drive), the device should be encrypted and kept locked away securely when not being used.

h. Data containing personal information should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud storage services**.

i. Servers containing personal information should be **sited in a secure location**, away from general office space.

j. Data containing personal information should be **backed up frequently**. Those backups should be tested regularly, in line with MOCA’s standard backup procedures.

k. Data containing personal information should **never be saved directly** to laptops or other mobile devices like tablets or smart phones. If a laptop or other mobile device contains individuals’ private information, it must be encrypted so that users cannot not
download any software or change the security settings without approval from the chief technology officer.

l. Staff must be mindful of security when traveling. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If a laptop must be left in a car, it should be locked in a trunk.

m. All servers and computers containing personal information data should be protected by approved security software and a firewall. Regularly run up-to-date anti-malware programs on individual computers and on servers on the network.

n. Avoid storing individuals’ personal information on any computer with an internet connection unless it is essential for conducting MOCA business.

o. Staff should not download unauthorized software. Software downloaded to devices that connect to MOCA’s network (computers, smartphones and tablets) could be used to distribute malware.

p. Staff should encrypt individuals’ personal information that MOCA sends to third parties over public networks (e.g., the internet) and encrypt sensitive information that is stored on MOCA’s computer network, laptops or portable devices used by Staff.

3. **Data Use**

a. Individuals’ private information may only be used for the purposes for which they are collected and processed. For example, use Social Security numbers only for required and lawful purposes such as reporting employee income to the Internal Revenue Service or administering employee benefits. Do not use Social Security numbers unnecessarily – for example, as an employee or customer identification number.

b. When working with individuals’ private information, staff should ensure the screens of their computers are always locked when left unattended.

c. Individuals’ private information should not be shared informally. In particular, it should never be sent by email. Unencrypted email is not a secure way to transmit information. Staff should not transmit private information such as Social Security numbers, passwords and account information, via email.
d. Data containing individual private information must be encrypted before being shared electronically. The IT manager can explain how to send data to authorized external contracts using encryption.

e. Staff should not save copies of personal information to their own computers. Always access and update the central copy of any data.

4. Data Accuracy

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

a. Data containing personal information should be stored or maintained in as few places as necessary. Staff should not create any unnecessary additional data sets.

b. Staff should take every opportunity to ensure individuals’ private information is updated. For instance, by confirming a customer’s details when they call or visit.

c. Data containing individuals’ private information should be updated as inaccuracies are discovered. For instance, if an individual can no longer be reached on their stored telephone number, it should be removed from the database.

5. Archiving / Disposal of Data

a. To ensure that individuals’ private information is kept for no longer than necessary, MOCA shall review and revise, if necessary, its existing document retention and destruction policy for each area in which individuals’ private information is processed and review that policy annually.

b. The document retention and destruction policy shall consider what data should/must be retained, for how long, and why. For example, donor data will be archived for no less than seven years for audit purposes. Within a reasonable amount of time thereafter, such data will be removed and permanently erased and/or deleted.

B. Additional Responsibilities

In addition, the following people have particular areas of responsibility regarding data protection:

1. The board of directors is ultimately responsible for ensuring that MOCA meets its legal obligations in connection with the implementation of reasonable data security protections.
2. The **chief technology officer** is responsible for:
   a. Keeping the board updated about data protection and responsibilities, risks and issues.
   b. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
   c. Arranging data protection training and advice for the people covered by this policy.
   d. Handling data protection questions from staff and anyone else covered by this policy.
   e. Dealing with requests from individuals to see the data MOCA holds about them (also called ‘subject access requests’).
   f. Checking and approving any contracts or agreements with third parties that may handle individuals’ private information and other sensitive data owned by MOCA.
   g. Ensuring all systems, services and equipment used for storing data meet reasonable security standards.
   h. Performing regular checks and scans to ensure security hardware and software is functioning properly, including installing necessary patches and updates.
   i. Evaluating any third-party services MOCA is considering using to store or process data.

3. The **President** is responsible for:
   a. Approving any data protection statements attached to communications such as emails and letters.
   b. Addressing any data protection queries from journalists or media outlets like newspapers.
   c. When necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

IV. **Privacy Notice**

MOCA shall post a privacy notice in the form of **Exhibit B** on its website and MOCA will review it periodically to ensure that it accurately reflects MOCA’s treatment of individuals’ private information.
V. Vendor Policy

A. Before outsourcing any of MOCA’s business functions such as payroll, web hosting, customer call center operations, data processing, or the like, MOCA should investigate the company’s data security practices and compare their standards to that of MOCA. If possible, a MOCA representative should visit their facilities.

B. When MOCA transfers individuals’ private information to a vendor, such as the Third Party Enterprise Platform Provider, for processing and/or storage, the data will be delivered over encrypted internet connections via Terminal Services.

1. Where the processing of data is outsourced to a vendor, as with the Third Party Enterprise Platform Provider, the vendor shall agree in a binding contract that the vendor will promptly notify MOCA of (a) any unauthorized access of any computerized data that compromises the security, confidentiality or integrity of MOCA Data (including any personally identifiable or sensitive information such as names, social security numbers, driver's license numbers, credit card or other account numbers, and other similar information, stored or processed on behalf of License Holder), (b) any failure by the vendor to comply with any applicable laws, or (c) any event that will require the vendor or MOCA to take any actions (including providing notices) under any applicable laws.

2. The vendor must also agree that if the vendor discovers or is notified of a material breach or potential material breach of the security of any MOCA Data, the vendor will immediately (i) notify MOCA of the same, and (ii) the vendor will investigate the breach or potential breach.

VI. Breach of the Security System

A. MOCA shall have a plan in place to respond to security incidents. The chief technology officer will coordinate and implement the response plan.

B. If a computer is compromised, it must be disconnected immediately from the network.

C. MOCA shall investigate security incidents immediately and take steps to close off existing vulnerabilities of threats to private information.

D. In the event of a breach of the security of the system, MOCA shall disclose any breach following discovery or notification of the breach to any New York resident whose private information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.
1. If notice of the breach is made to affected persons, notice shall also be provided to the New York State Attorney General, the Department of State and the Division of State Police.

2. Notice to affected persons is not required, however, if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and MOCA reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, MOCA shall provide the written determination to the New York State Attorney General within 10 days after the determination.

END OF POLICY
APPENDIX A

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Articles 12 through 23 of the GDPR set out certain requirements related to the rights of data subjects. Generally, these primary rights include:

a. the right to access;

b. the right to rectification;

c. the right to erasure;

d. the right to restrict processing;

e. the right to object to processing;

f. the right to data portability;

g. the right to complain to a supervisory authority; and

h. the right to withdraw consent.
Thank you for choosing to be part of the Museum of Chinese in America community. We work hard to build and maintain a relationship of trust with you. So, when it comes to handling your information, we do so carefully and sensibly, and in ways that live up to that trust. This policy lets you know how we do that, including what information we collect, how we use and protect it, and how you can decide what we do with it. We hope you take some time to read through this policy carefully, as it is important. If there are any terms in this policy that you do not agree with, please discontinue use of our sites and our services.

This privacy policy applies to all information collected through our website (such as www.mocanyc.org), and any other related services, sales, marketing or events (we refer to them collectively in this privacy policy as the “Services”).

**TABLE OF CONTENTS**

What We Collect

How We Collect Your Information

How We Use Your Information

How We Safeguard Your Information

How and When We Share Your Information

What We Share

How Long We Keep Your Information

Your Rights and Choices

-EU Residents
Here’s a short introduction to our privacy practices:

**WHAT WE COLLECT**

- Information you give us. We collect personal information that you provide to us such as name, address, contact information, password and security data, and payment information.

- Information we collect when you contact us, visit our sites, visit our museum when expressing an interest in obtaining information about us or our products and services, participating in activities on the Services or otherwise contacting us.

- Information – such as IP address and/or browser and device characteristics – is collected automatically when you visit our sites.

- Information we get from other companies who have obtained your consent to share or sell it or have ensured that other companies from whom they have received your information can share it with them and, in turn, with us and/or other companies.

We may combine any and all of this information to help create better products, services, and user experiences.

**HOW WE COLLECT YOUR INFORMATION**

We collect information about you in many ways from many places. Some of the information we collect may include personal information that can be used to
identify you; for example, your name, email address, telephone number, or postal address.

Please note: We may combine all of the information we collect about you to give you better products, services, and user experiences.

- **You provide it to us.** You give us your information when signing up for an account on our websites or in mobile apps or by calling or emailing us. We may ask for things like your name, email or home address, date of birth, payment information, your age, gender, the number of people in your family, and the way you want us to send you information about our products and services—for example, to your home address, email address, or by texting you.

- **From sites and emails.** We may use technologies that automatically collect information when you visit our sites, view our advertisements, or use our products or services. For example, we use cookies (a tiny file stored on your computer’s browser) to tell us what browser and operating system you are using, your IP address, web pages you visit, links you click, or whether you have or have not opened an email from us.

- **From other places.** We may get information that other companies share with or sell to us. For example, you may have given consent for another company to share your personal information with us when you signed up for telecom services or a retailer loyalty points program. We may also collect information from places that you know everyone can see, such as from internet postings, blog entries, videos, or social media sites. We may also receive information from other companies who are in the business of collecting or aggregating information about you sourced from publicly available databases or from consent you have given to their use and subsequently our use of your information.

**HOW WE USE YOUR INFORMATION**

- Send you the products and services you ask for.

- Send you marketing and promotional communications relating to MOCA’s current and upcoming exhibitions, programs and events.
• Tell you about our and our marketing partners’ products and services.
• Help us run our sites and services.
• Enforce our terms, conditions and policies for business purposes, legal reasons and contractual obligations.
• Respond to legal requests and prevent harm.
• Respond to user inquiries/offer support to users.

To protect your privacy, we will use the least amount of information we can to accomplish the task at hand, put measures in place to prevent mixing information in ways that would allow cookie and device IDs to specifically and directly identify you (e.g., by name), and delete your information when we no longer need it for our business purposes.

HOW WE SAFEGUARD YOUR INFORMATION

We respect your personal information and take steps to protect it from loss, misuse, or alteration. Where appropriate, these steps can include technical measures like firewalls, intrusion detection and prevention systems, unique and complex passwords, and encryption. We also use organizational and physical measures such as training staff on data processing obligations, identification of data incidents and risks, restricting staff access to your personal information, and ensuring physical security including appropriately securing documents when not being used.

HOW AND WHEN WE SHARE YOUR INFORMATION

• When we have your consent and only for the purpose to which you have agreed.
• With other companies such as vendors, consultants and other third–party service providers we hire to help us run our business.
• To help us protect our rights or property, e.g., fraud prevention or information security.
• When required by law or government authorities.
- When we have entered into a contract with you, we may process your personal information to fulfill the terms of our contract.

**WHAT WE SHARE**

**With Other Companies and/or Non-Profit Organizations.** When we have your consent, we may share your information with select partners so they can send you offers, promotions, or ads about products or services we believe you may be interested in. We do not sell your personal information to marketers.

**With Service Providers.** We may need to share your information with companies who help us run our business, including hosting our sites, delivering our emails to you, analyzing the data we collect, and sending you the products and services you requested. We share only the personal information needed for these companies to complete the tasks we request. They are required to protect your information in the same way we do and will not share it or use it for any other purpose.

**Other Situations.** We may share your information with companies who help us protect our rights and property, or when required by law or government authorities.

**HOW LONG WE KEEP YOUR INFORMATION**

We will only keep your personal information for as long as necessary to fulfill the purposes outlined in this privacy policy unless otherwise required by law (such as tax, accounting or other legal requirements). When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or if this is not possible, then we will securely store your personal information and isolate it from any further processing until deletion is possible.

**YOUR RIGHTS AND CHOICES**

**Marketing.** You can tell us to stop sending you email and text messages by following the opt-out instructions sent with these communications. You can also choose to stop receiving marketing email, SMS, or postal mailings by clicking here. While we will honor your choices, we may need to keep
information to do so. For example, if you tell us to stop sending marketing emails, we will need your email address on file so that our systems remember that you no longer wish to receive marketing communications to that email address.

**European Union Residents.** If you live in the EU, you may access the personal data we hold about you, request that inaccurate, outdated, or no longer necessary information be corrected, erased, or restricted, and ask us to provide your data in a format that allows you to transfer it to another service provider. You also may withdraw your consent at any time where we are relying on your consent for the processing of your personal data. And you may object to our processing of your personal data (this means ask us to stop using it) where that processing is based on our legitimate interest (this means we have a reason for using the data) and we will no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing. If you would like more information about data protection and your personal data rights in general, please visit the European Data Protection Supervisor’s site at https://edps.europa.eu/data-protection/. If you are not happy with our response to your requests, you may lodge a complaint with the data protection authority in your country. If you would like to make a subject access, please contact us [here](#).

**California Residents.** If you are a resident of California, you have the right to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with whom we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us by contacting us [here](#).

**Children’s Online Privacy.** We follow all applicable data protection laws when collecting personal information online from children. We do not knowingly collect children’s private information online.
COOKIES

Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services on our website.

SITE AND APP CONTENT

Plugins. Our websites may include plugins from other companies such as social networks. An example of a plugin is the Facebook “Like” button. These plugins may collect information (e.g., the URL of the page you visited) and send it back to the company that created them. This may happen even if you do not click on the plugin. These plugins are governed by the privacy policy and terms of the company that created them, even though they appear on our sites.

Logins. Our websites may allow you to log in using your account with another company such as, for example, “Login with Facebook.” When you do this, we will have access only to the information that you have given us consent to receive from your account settings in the other company’s account you’re using to log in with.

User Content. Some of our sites and apps will allow you to upload your own content for blogs, videos, and other functions. Please remember that any information you submit or post becomes public information. We do not have control over how others may use the content you submit to our sites and apps. We are not responsible for such uses in ways that may violate this privacy policy, the law, or your personal privacy and safety.

POLICY UPDATES

We may update this privacy policy from time to time. The updated version will be indicated by an updated “Revised” date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy policy frequently to be informed of how we are protecting your information.
CONTACT US

Please contact privacy@mocanyc.org directly with any questions or concerns you may have about your privacy and our data protection practices.