MUSEUM of RICHMOND

Old Town Hall • Whittaker Avenue • Richmond • Surrey TW9 1TP
Telephone 020 8332 1141 • Email info@museumofrichmond.com

Information Security Policy

Incorporating Data Protection

Date created: December 2019
Version: 2.4
Last reviewed: May 2021
Review due: May 2023
Lead person: IT Trustee (in discussion with Curator and Executive Officer)

ACCREDITED MUSEUM

ARTS COUNCIL ENGLAND

Arts Council England Registered Museum no. 80
The Museum of Richmond is a company limited by guarantee
Registered no. 2048888. Charity Registered no. 295164

MUSEUM of RICHMOND

Information Security Policy

Contents

1: Definitions

1.1: Personal Data is covered by Data Protection legislation. This includes: postal addresses; telephone numbers; email addresses; financial information (e.g. donations and subscriptions); HR information (e.g. staff reviews and CVs). A more comprehensive definition can be found on the ICO website at the link below:

https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

1.1.1 There is a register of personal data which can be found at the end of this document.

1.2: The **Data Subject** is the individual about whom information is held.

1.3: The **Data Controller** determines the purposes for which and the manner in which any personal data are, or are to be, processed. This is often the Board of Trustees for a charity

1.4: The **Data Processors** are any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

1.5: The **IT Trustee** is the Board member with specific responsibility for the use of IT in the Museum.

2: Information Security

2.1: Access and Authentication Controls

2.1.1: All computers used in the Museum require a user account and password to logon. There are no Guest accounts

2.1.2: Passwords are changed every 180 days and are complex, including upper and lower case letters and numbers

2.1.3: User accounts are role-based. The Curator and Learning and Audience Development Officer have their own personal accounts; other users – volunteers, interns, young curators, work experience placements – have shared role-based accounts (e.g. MORIntern)

2.1.4: There is an administrator account on each computer, the password for which is known to the Curator, Learning Officer and the IT Trustee

2.1.5: Access to data is controlled through authentication belonging to the user accounts. This is configured as follows:

2.1.5.1: **Personal** folders accessible only to that user account and the administrator; this includes Outlook information.

2.1.5.2: **Public** folders accessible to all user accounts.

2.1.5.3: **Private** folders accessible only to the curator, learning officer and administrator.

2.1.5.4: **Archive** folders accessible only to the curator, learning officer and administrator.

2.1.6: All personal data is stored in the Private folders

2.1.7: There are also passwords associated with each of the Outlook email accounts. These should also be complex and not shared

2.1.8: Personal data is also held in eHive, the collection management system and MailChimp, the service we use to send out emails. In both cases there is a single username and password held by the Curator and Learning Officer. Personal data is also held in Art Tickets, an online ticketing system provided by the Art Fund. To access this information, the Curator, Learning Officer and Museum Assistant have individual Art Fund accounts with independent usernames and passwords

2.1.9: Some information relating to the Museum, including personal data, is also held on the Treasurer's computer. This must be a computer for his/her sole use and protected by a user account and complex password, appropriate security software and backup systems

2.1.10: A remote access system is installed on Museum laptops. This is password protected and the same user accounts apply. Staff do not transfer personal data from Museum computers and laptops to their own personal devices

2.2: Backup

2.2.1: All the files stored in the personal, public, private and archive folders are backed up off-site each day (excluding Sunday). Retention of backups is indefinite, although some files and folders may be permanently deleted in order to save storage space.

2.3: Protection against External Threats

2.3.1: All the computers have Norton 360 installed. This includes a firewall together with anti-virus and anti-spam protection. The software is automatically updated and scans performed on each computer are scheduled to take place at least once a week.

2.3.2: Only the administrator account has full administrative privileges on each computer to reduce the risk of harmful software being installed.

2.3.3: The Museum itself is protected by a locked door and an alarm system. The only key holders are permanent staff members and a Board member who is local to the Museum. On occasions Board members and such temporary personnel as may be required to cover the absence of permanent staff may hold keys for a brief time. There is also a set of keys held by the Council in case of emergency.

2.3.3: Any paper documents which contain personal information are held in a locked cupboard for which only the Curator and Executive Officer and the Learning and Audience Development Officer have keys.

2.3.4: The Wi-Fi router used by the Museum's laptops is secured by an access key with encryption.

2.3.5: No computers other than those owned by the Museum, or explicitly approved by the IT Trustee, may be connected to the local area network.

2.4: Computer Use Policies

2.4.1: The computers are only to be used for purposes related to the Museum

2.4.2: Passwords are not to be shared except where the account itself is shared (e.g. between the volunteers)

2.4.3: Passwords are to be changed in a systematic fashion every 180 days and should always be complex

2.4.4: Personal data is not to be transmitted off-site either by email or through the use of removable media

2.4.5: Personal data should not be passed to any 3rd Party, with the exception of:

2.4.5.1: Payroll agency – necessary information for staff members only

2.4.5.2: HMRC – information required for PAYE

2.4.5.3: Companies House – information required relating to the Directors

2.4.5.4: Charity Commission – information required relating to the Trustees

2.4.5.5: Museum's bank – information required relating to account signatories

2.4.5.6: NHS Test and Trace – if information required and requested by Public Health England to support contact tracing during the Covid-19 pandemic

2.4.6: Any breaches in security or warning messages generated by the computers should be notified immediately to the IT Trustee

3: Data Protection

3.1: Roles

3.1.1: Data Controller

3.1.1.1: The Board of the Museum acts as the data controller. Specific responsibilities are held by:

3.1.1.1.1: IT Trustee – overall management of Data Protection compliance

3.1.1.1.2: Learning and Audience Development Officer – day-to-day responsibility for ensuring that personal data is handled appropriately, in accordance with this policy

3.1.2: Data Processors

3.1.2.1: The data processors are any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Role/Person	Data Processor?	Note
Curator	No	Employees are not data processors
Learning Officer	No	Employees are not data processors
Other paid staff	No	Employees are not data processors
Volunteers	No	Volunteers working for the Museum are not data processors
Board members	No	Volunteers working for the Museum are not data processors
Payroll agency	Yes	

3.2: Policy

3.2.1: Only personal data which is essential to the specific purpose should be retained. In the case of volunteers, Patrons and Board members this is limited to contact information. For Friends this is extended to a record of subscriptions and donations

3.2.2: Sensitive personal data (as defined by GDPR legislation) should not be retained without the consent both of the data subject and any requirement for this should first be agreed with the IT Trustee. This data is collected through visitor Feedback Forms, which are collated into spreadsheets and the original forms shredded with no way to trace back to the individual. Friends diversity data is also collected, collated separately from identifying information and then shredded. During the Covid-19 pandemic, Feedback Forms are sent and received electronically, and the same procedures apply

3.2.3: Duplication of personal data should be avoided so far as possible. For example, email distribution lists should only be stored within the Mail Chimp system

3.2.4: Personal data which is deemed to be "inactive" will not be retained for more than 5 years past the last active use. For example, information about a supporter whose membership has lapsed will not be retained for more than 5 years

3.2.5: Personal data will be updated whenever information is received that indicates a change

3.2.6: Paper records containing personal data will be kept in a locked, secure location and will be subject to the same retention rules as electronic data. Accession records and entry paperwork are retained indefinitely and are kept in a locked filing cabinet – to which only the Curator has access

3.2.7: Paper records which reach their retention date will be shredded and disposed of appropriately

3.2.8: Any subject access request will be referred immediately to the Board

3.2.9: Communication to specific individuals regarding the activities of the Museum, including any fundraising requests will be controlled as follows (in accordance with the Privacy and Electronic Communications Regulations):

3.2.9.1: Friends will be given the opportunity to opt out of such communications at the time of becoming a Friend or on the annual renewal

3.2.9.2: Every email that is sent to either paid-up supporters or those who have expressed a wish to be kept informed about the Museum will include the facility to opt out of any future communications

3.2.9.3: Telephone calls will only be made in response to specific requests for information

3.2.9.4: It is assumed that Board members and Patrons are content to receive communications from the Museum

3.2.9.5: A privacy statement is available on the Museum website outlining the purposes for which personal data is kept

4: Museum of Richmond Privacy Policy

4.1: We are committed to protecting the privacy and the confidentiality of the personal information of visitors, supporters and volunteers. We undertake to ensure that all personal information in our possession is processed in accordance with the principles of the Data Protection Act 1998.

4.2: We collect personal information (your name and contact details) that you supply to us. Your information is collected when you make loans of Museum artefacts, request information from us, join one of our Friends or supporters schemes, contact us or make a booking with us. We will update your information whenever we get the opportunity to keep it current, accurate and complete.

4.3: Any information you provide will be used for the Museum's purposes only. We will not pass on your information to any third party unless required by law or regulatory obligations. The information will be used to allow us to keep you informed about events and exhibitions at the Museum. It may also be used in fundraising communications.

4.4: You may indicate your preference for receiving direct marketing by telephone or email from us. You will be given the opportunity on every communication we send you to indicate that you no longer wish to receive our direct marketing material. Once properly notified by you, we will take steps to stop using your information in this way.

4.5: Credit or debit card information provided when purchasing tickets or other items from us or intermediaries such as Eventbrite is not stored by us.

4.6: You have the right to ask in writing for a copy of the information we hold about you and to correct any inaccuracies in your information.

5: Register of Personal Data

5.1: Electronic Sources

Data subjects	Information held	Where	Justification for holding data [1]
Permanent staff	Name, address, contact details	Private folders Treasurer's computer	Contract
	Payroll information	Payroll agency (external) system Treasurer's computer	Contract
	Staff reviews	Private folders	Legitimate interest Contract
	CVs	Private folders	Legitimate interest
	Formal staff communications	Private folders Treasurer's computer (where relevant)	Contract Legal
Temporary (paid) staff	Name, address, contact details	Private folders	Contract
	Payroll information	Payroll agency (external) system Treasurer's computer	Contract
Volunteers	Name, address, contact details	Private folders	Legitimate interest Consent
Friends (belonging to membership scheme)	Name, address, contact details	Friends database/spreadsheet in Private folders	Legitimate interest
	Payments made to scheme	Treasurer's computer (accounts) Friends database/spreadsheet and monthly accounts spreadsheet in Private folders	Legitimate interest
	Email address	Friends database/spreadsheet in Private folders	Consent

[1] See Lawfulness of Processing Conditions

Donors (financial)	Donations made by cheque or direct bank transfer	Treasurer's computer (accounts) Monthly accounts spreadsheet in Private folders	Legitimate interest
	Names, address, contact details (where supplied by the donor, including anyone who gives via CAF Donate)	Donor database/spreadsheet in Private folders	Legitimate interest
	Gift Aid forms including name and address	Treasurer's computer (for making Gift Aid claims)	
Donors of loaned or gifted artefacts	Names, address, contact details (where supplied by the donor)	eHive data repository	Legitimate interest
Visitors (for the period during which the Museum operates an online ticketing system)	Name, address, contact details	Art Tickets. This data is not transferred to Museum folders	Legitimate interest
Visitors who cannot check-in to NHS Test and Trace using the app and must manually leave their contact details (for the period during which NHS Test and Trace is in operation)	Name and telephone number; or email address or postal address if no available contact number	Spreadsheet in private folders. All data records of this type are destroyed 21 days after collection, in accordance with government regulations	Legal requirement – to support NHS Test and Trace during the Covid-19 pandemic
Event attenders	Email address	Updated in Mail Chimp system – no records kept once uploaded; can unsubscribe	Legitimate interest

		Eventbrite bookings – no personal information is held on our systems	
Board members	Name, address, contact details	Private folders	Consent
Patrons	Name, address, contact details	Private folders	Legitimate interest
Benefactors	Name, address, contact details Records of donations	Private folder Treasurer's computer (accounts)	Legitimate interest
Marketing Contacts	Name, address, contact details	Private folder	Consent

5.2: Paper Sources

Data subjects	Information held	Justification for holding data [2]
Friends	Name, address, contact details on original application and renewal forms. These are scanned and shredded so only retained very briefly in paper form	Legitimate interest
Volunteers	Name, address, contact details and other information provided on application forms	Legitimate interest
Donors	Gift Aid forms including name and address	
Visitors and participants in events and workshops, notably children	Photo permission forms. These are scanned and shredded once completed so only retained very briefly in paper form	Legal
Visitors who cannot check-in to NHS Test and Trace using the app and must manually leave	Name and telephone number; or email address or postal address if no available contact number. This information is transferred to a spreadsheet at the end of every day and paper forms are shredded, so	Legal requirement – to support NHS Test and Trace during the Covid-19 pandemic

[2] See Lawfulness of Processing Conditions

their contact details (for the period during which NHS Test and Trace is in operation)	only retained very briefly in paper form	
	Feedback forms These are entered into our systems with any personal information removed and then shredded.	Legitimate interest
Object donors	Paperwork associated with artefacts loaned or gifted to the Museum	Legitimate interest

5.3: Lawfulness of Processing Conditions

5.3.1: **Consent** of the data subject

5.3.2: Processing is necessary for the performance of a **contract** with the data subject or to take steps to enter into a contract

5.3.3: Processing is necessary for compliance with a **legal** obligation

5.3.4: Processing is necessary to protect the **vital interests** of a data subject or another person

5.3.5: Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller

5.3.6: Necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject