Museum of Richmond

Information Security Policy

Incorporating Data Protection

Version 1.3, 23rd January 2017

Contents

Definitions

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/

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

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

The **Data Controller** determines the purposes for which and the manner in which any personal data are, or are to be, processed.

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

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

Information Security

Access and Authentication Controls

- All computers used in the Museum require a user account and password to logon. There are no Guest accounts
- Passwords are changed every 120 days and are complex, including upper and lower case letters and numbers
- User accounts are role-based. The curator and learning officer have their own personal accounts; other users – volunteers, interns, young curators, work experience placements – have shared role-based accounts (e.g. MORIntern)
- There is an administrator account on each computer, the password for which is known to the curator and the IT Trustee
- Access to data is controlled through authentication belonging to the user accounts. This is configured as follows:
    - **Personal** folders accessible only to that user account and the administrator; this includes Outlook information
    - **Public** folders accessible to all user accounts
    - **Private** folders accessible only to the curator, learning officer and administrator
    - **Archive** folders accessible only to the curator, learning officer and administrator
- All personal data is stored in the Private folders
- There are also passwords associated with each of the Outlook email accounts. These should also be complex and not shared
- 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

Backup

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.

Protection against External Threats

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.

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

The Museum itself is protected by a locked door and an alarm system. The only key holders are permanent staff members, Board members and such temporary personnel as may be required to cover the absence of permanent staff.

Any paper documents which contain personal information are held in a locked cupboard for which only the Curator, Learning Officer and Projects Officer have keys.

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

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

Computer Use Policies

- The computers are only to be used for purposes related to the Museum
- Passwords are not to be shared except where the account itself is shared (e.g. between the volunteers)
- Passwords are to be changed in a systematic fashion every 120 days and should always be complex
- Personal data is not to be transmitted off-site either by email or through the use of removable media
- Personal data should not be passed to any 3rd Party, with the exception of:
    - Payroll agency – necessary information for staff members only
    - HMRC – information required for PAYE
    - Companies House – information required relating to the Directors
    - Charity Commission – information required relating to the Trustees
    - Museum's bank – information required relating to account signatories
- Any breaches in security or warning messages generated by the computers should be notified immediately to the IT Trustee

Data Protection

Roles

Data Controller

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

- IT Trustee – overall management of Data Protection compliance
- Learning officer – day-to-day responsibility for ensuring that personal data is handled appropriately, in accordance with this policy

Data Processors

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	

Policy

- 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 supporters this is extended to a record of subscriptions and donations
- 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
- 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
- Personal data will be updated whenever information is received that indicates a change
- 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
- Paper records which reach their retention date will be shredded and disposed of appropriately

- Any subject access request will be referred immediately to the Board
- Communication to specific individuals regarding the activities of the Museum, including any fundraising requests will be controlled as follows:
    - Supporters will be given the opportunity to opt out of such communications at the time of becoming a supporter or on the annual renewal
    - 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
    - Telephone calls will only be made in response to specific requests for information
    - It is assumed that Board members and Patrons are content to receive communications from the Museum
    - A privacy statement is available on the Museum website outlining the purposes for which personal data is kept

Museum of Richmond Privacy Policy

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.
2. We collect personal information (such as your name and contact details) that you supply to us. Your information is collected when you request information from us, join our supporters' scheme, 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.
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. 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.
5. Credit card information provided when purchasing tickets from us or intermediaries such as Eventbrite is not stored by us.
6. You have the right to ask in writing for a copy of the information we hold about you (for which we may charge a fee) and to correct any inaccuracies in your information.

Register of Personal Data

Electronic Sources

Data subjects	Information held	Where
Permanent staff	Name, address, contact details	Private folders Treasurer’s computer
	Payroll information	Payroll agency (external) system Treasurer’s computer
	Staff reviews	Private folders
	CVs	Private folders
	Formal staff communications	Private folders Treasurer’s computer (where relevant)
Temporary (paid) staff	Name, address, contact details	Private folders
	Payroll information	Payroll agency (external) system Treasurer’s computer
Volunteers	Name, address, contact details	Private folders
Supporters (belonging to membership scheme)	Name, address, contact details	Supporter database/spreadsheet in Private folders
	Payments made to scheme	Treasurer’s computer (accounts) Supporter database/spreadsheet and monthly accounts spreadsheet in Private folders
Donors	Donations made by cheque or direct bank transfer	Treasurer’s computer (accounts) Monthly accounts spreadsheet in Private folders
	Names, address, contact details (where supplied by the donor)	Donor database/spreadsheet in Private folders
Event attenders	Email address	Updated in Mail Chimp system – no records kept once uploaded
Board members	Name, address, contact details	Private folders
Patrons	Name, address, contact details	Private folders

Paper Sources

- Supporters original forms
- Volunteers information
- Photo permission forms