CAMBRIDGE MUSEUM OF TECHNOLOGY
The Old Pumping Station, Cheddars Lane, Cambridge, CB5 8LD

Charitable Incorporated Organisation Number 1156685

Data Management Policy

Introduction

The General Data Protection Regulation (GDPR) 2018 comes into force on 25 May 2108. It will be supplemented by the Data Protection Bill, currently being considered by Parliament, and replace the 1998 Data Protection Act (DPA). GDPR sets out EU wide measures for data handling and protection. The Information Commissioner's Office has also stated that whether the UK leaves the EU or not GDPR will still apply.

The Privacy Notice and Data Retention policy deals with the specifics of complying with the GDPR. This policy deals with how to manage those policies and their compliance requirements. It also covers the handling of non GDPR data.

This policy sets out how personal data acquired by us should be processed, stored and deleted when no longer required for both paper and digital records. Personal data also includes images, audio/video and photographs where individuals can be identified. CCTV is also included but different requirements apply – see separate CCTV notice.

All processors and users of personal information, including the Board of Trustees, Management Committee, staff and volunteers are obliged to comply with the GDPR and new Data Protection Act. People handling personal data at the museum must therefore be made aware of GDPR and the new Data Protection Act, when it comes into force and have been trained.

Note for electronic communications, mostly email and text, the Privacy and Electronic Communications Regulations (PECR) also apply.

GDPR Data Protection Principles

GDPR controls how personal information is used by organizations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles' and ensure the information is:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- Accurate and where necessary kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a way that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Roles and Responsibilities

Data Controller and Data Processor

A Controller determines the purposes and means of processing personal data. The Museum "We" is the Data Controller, not an individual at the museum. A trustee has been appointed to oversee the museum's compliance with the regulation and govern the work of both internal staff, volunteers and external Data Processors. The Controller decides how and why the data is processed and is responsible for, and is able to demonstrate compliance with Data Protection, so all reports, audits etc. should be sent to the appropriate trustee, who in turn will report to the Board of Trustees. It is recommended any decisions taken by the trustees be minuted for audit purposes.
The Data Controller i.e. the Board of Trustees are accountable for Data Policies and for ensuring compliance with them.

Note a processor has a very distinct meaning under the GDPR. This refers to a person or body who is separate from the data controller i.e. not an employee or a volunteer and who processes personal data on behalf of the data controller i.e. the Museum. In other words, the controller gives the processor a specific job to do – and the processor does it.

We are in effect both controller and processor and, in addition, use 3rd party processors.

Both the controller and processor have legal obligations set out in the Regulation.

> "If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
>
> However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR."

Data Protection Officer

The GDPR describes the responsibilities and duties of a Data Protection Officer (DPO) - see Information Commissioner's Office (ICO) Guide. It is not compulsory for us to appoint a DPO but we can share a DPO with other organizations on a voluntary basis.

Quote from the ICO guide:
"Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can be seen to play a key role in your organisation's data protection governance structure and to help improve accountability.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle."
It is, therefore, recommended we appoint a DPO on a shared basis with other organizations to carry out the tasks described in the GDPR. The main ones are listed below:

The DPO's tasks are defined in Article 39 of GDPR as:

- To inform and advise you and your employees *including volunteers* about your obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff *and volunteers,* and conducting internal audits;
- To advise on, and to monitor, data protection impact assessments;
- To cooperate with the supervisory authority; and
- (To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).) – *not in our case, only for full time DPO*

It's important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under GDPR Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

Data Processing

We can collect and process data on a lawful basis provided one or more of the criteria listed in the regulation has been met. These criteria are:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose. This applies to individuals who can be recognised from Photos & Moving Images

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Note -This cannot apply if you are a public authority processing data to perform your official tasks.
The attached Data Collection Schedule lists the processing tasks we or our third party processors undertake and the lawful justification for doing so.

It is essential to link each element of personal data collection to one of the above categories and allow public access to this. The information required is included in the Data Retention Policy.
We must keep a record of when and how we got consent from the individual.
We must keep a record of exactly what we told them at the time.

The ICO recommends all data should be stored digital where possible on a secure basis.

Third Party Data Processors

We use third party data processors for a number of tasks e.g. Just Giving for donations and MailChimp for bulk emailing. For a full list see our Privacy Policy
These organisations working on our behalf are approved data processors for the Cambridge Museum of Technology and we are responsible for the work they do on our behalf.
As they must comply in their own right with the Regulation we too have a responsibility to comply with their requirements and to monitor and record any changes they make e.g. changes to their Privacy Policy or Notice. We should, therefore, regularly audit the arrangements.
If a third party e.g. Just Giving supplies us with an individual's personal data we are obliged to send that individual as soon as possible, and in any event within one month, our Privacy Notice.
We must also update our records if we are notified by a third party of a change in an individual's person information, consent conditions etc.
If advised by a third party they have agreed with an individual to exercise their "right to be forgotten" then we must contact the individual to see if they wish to exercise this right with us.

If these processors are based outside of the EU and in countries where there is no equivalent data protection laws e.g. MailChimp (USA) then we must have the express consent of the person whose data we wish to process before sending it to these processors.
A full list of Third party processors other than those relating to staff payroll and pensions is included in our Privacy Notice.

The museum does not disclose personal data to any third party or external organisation, other than data processors carrying out work on our behalf and acting on our instructions. We have contracts with these organisations.
Data will never be passed or sold to any third party for any other purpose.

Data Protection Impact Assessments (DPIA)

The trustees should carry out a DPIA on our current Data Processing activities prior to the implementation of GDPR in May 2018.
Before implementing any major change in Data Processing collection, processing or storage in future a DPIA should be carried out.
To assist in this evaluation the ICO DPIA checklist and assessment template is included in the Checklist GDPR in Dropbox/Data Protection.

Individual's Rights

These rights are spelt out in more detail in the Museum's privacy policy.
All data along with the appropriate justification must be recorded. Where consent is given then they must be an easily available opt-out to withdraw their consent should they wish to.

An Individual Requesting or Correcting their Information (Subject Access Request)

As stated in the Privacy Notice and individual has the right to ask us if we are keeping any personal data about them and to request a copy of that personal data. They can also ask us to correct any data they feel is incorrect.
To make a subject access request they must provide adequate proof of identity such as a copy of their passport, birth certificate or driving license before their request can be considered. There will be no charge for the request, in accordance with GDPR, unless the request is 'manifestly unfounded or excessive' or if you make multiple requests.
Once we have received their request, the agreed fee if required, and proof of identity they must receive a response from the museum within one month and they must receive copies of any information we hold on them. Exemptions to disclosure may apply in some circumstances- see ICO guidance.

As stated in the Privacy Notice requests should be sent to the Curator at the museum's address.

The individual's right to erasure or 'the right to be forgotten'

An individual has a right to have their data erased under some circumstances. The right of erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and the museum can refuse to deal with a request. For more information contact the Curator.

Right of Complaint

If an individual wishes to complain about our treatment of their data they have the right to complain as detailed in the Privacy Notice. Such complaints should be handled promptly and must be completed within one month.

Non GDPR Data

The museum collects data, which falls outside GDPR categories. This data is mainly but not exclusively:

- Publicity, Newsletters. Leaflets sent out to local media, hotels, tourist attractions and other museums giving general information.
- Schools
- Premises hire on a commercial basis e.g. artists.
- Retailing including Shop activities.
- Third party events held on site.

Whilst these categories do not necessarily come under the regulation it is best practice, for example contacting schools, to contact the appropriate person(s) who are the agreed point of contact. See both our Privacy Notice and ICO guide.
If they then wish to opt out of any further communication then this request must be actioned and recorded.

Other Non GDPR data. Other Data should be managed in a similar manner to GDPR and should be included as non GDPR data in the Data Retention Policy.

Security

All reasonable steps must be taken to ensure that personal data is secure and we have implemented security procedures and technical measures to protect the personal data that we have under our control from:

- Unauthorised Access.
- Improper Use or Disclosure.
- Unauthorised Modification.

While we cannot ensure or guarantee that loss, misuse or alteration of data will not occur while it is under our control, we use our best efforts to try to prevent this.

The following measures are recommended to achieve the above:

- Access to computer files should be restricted using privilege levels and passwords.
- Regular password changes should be enforced and the number of attempted logins limited.
- The museums email addresses are to be used for all business operations.
- Equipment should be sited in a secure location where access can be restricted - the public and volunteers not involved in data processing should not be able to view terminal screens.
- Terminals should not be left unattended and should be logged-off at the end of a session: "log-off, switch off and lock up".
- Dedicated museum laptops, USB sticks etc. should only be used for museum activities.
- Redundant data should be wiped, overwritten or shredded and destroyed
- Data must be backed up and stored in an appropriate manner.
- Storage media should be locked up after use.
- For large amounts of sensitive data, we should consider keeping a copy in a fire-proof safe at a separate location.
- Network systems, Laptops, USB sticks etc. should be considered to be insecure. Data must be kept as secure as possible, using encryption, de-personalisation or anonymisation and password-protection if possible. If storing highly sensitive data is required then consider using stand-alone machines.
- Computer printout containing personal information should be stored as for paper files then shredded before disposal. It should not be used as scrap paper.
- Manual (paper) files must be stored securely. Data, especially sensitive data, should be stored in locked filing cabinets. Paper files should be shredded before disposal

Changes to the Data Management Policy

As with the Privacy Policy this policy must be periodically reviewed, at least annually, maximum of two years, and preferably with the help of an independent Data Protection Officer.
Any changes made should be recorded and the new policy filed securely along with the previous policy.