NATIONAL MUSEUMS NI

Data Protection Policy & Procedure

November 2021

Approved by: Senior Management Team October 2021

Approved by: The Board

Next Review Date: November 2024

1. Purpose of Procedure

National Museums NI is committed to ensuring that the personal information it manages conforms to the General Data Protection Regulation and Data Protection Act and these procedures outline the arrangements which the organisation has put in place to achieve this.

2. Procedure Drivers

- General Data Protection Regulation 2018
- Data Protection Act 1998
- Information Commissioners Office – guidance documents

3. Procedure owner / contacts

Head of Finance & Governance

1.0 General Data Protection Regulation

From 25 May 2018 the General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998, which was brought into law as a way to implement the 1995 EU Data Protection Directive. GDPR builds upon the principles established in the 1998 Act and seeks to give people more control over how organisations use their data. It also ensures data protection law is almost identical across the EU.

In the full text of GDPR there are 99 articles setting out the rights of individuals and obligations placed on organisations covered by the regulation. These include allowing people to have easier access to the data organisations hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people they collect information about. The steps being taken by National Museums NI to ensure compliance with GDPR are summarised in Appendix C.

2.0 Purpose of Procedures

National Museums NI is committed to ensuring that the personal information it manages conforms to the relevant legislation and it will take all reasonable steps to ensure that personal information is kept secure against unauthorised access, loss, disclosure or destruction.

National Museums NI needs to keep certain information about employees, volunteers, Trustees and users of our services to allow us to monitor performance, achievements, operational issues, management of the collections it holds and for health and safety purposes. We recognise that the lawful and correct treatment of personal data is very important to successful operations and to maintaining confidence between ourselves, the Northern Ireland Assembly, our partners and our visitors. Any personal data we collect, record or use in any way, whether it is held on paper, on computer or other media will have appropriate safeguards applied to it to ensure that we comply with legislative requirements.

To this end, National Museums NI fully endorses and adheres to the principles of data protection as set out in GDPR.

3.0 The Data Protection Principles

3.1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the following conditions has been met. Processing must be:

- with the consent of the data subject
- necessary for the performance of a contract with the data subject
- for the compliance with any legal obligation (other than contractual)
- to protect the vital interests of the data subject

- to carry out public functions
- to pursue legitimate interests of the data controller unless prejudicial to the legitimate interests of the data subject.

(b) in the case of sensitive personal data at least one of the conditions must be met. Processing must be:

- with the explicit consent of the data subject
- necessary to comply with the data controller's legal duty in connection with employment
- to protect the vital interests of the data subject or another person
- carried out by certain non-profit bodies
- where the information has been made public by the data subject
- in legal proceedings, to obtain legal advice, or exercise legal rights
- to carry out public functions
- for medical purposes
- for equality opportunities monitoring

3.2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

3.4. Personal data shall be accurate and, where necessary, kept up to date.

3.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

3.6. Personal data shall be processed in accordance with the rights of data subjects under the legislation.

3.7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3.8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4.0 Definitions

Data controller – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any person data are, or will be processed.

Data Subject – an individual about whom personal data is held.

Processing – this is any activity that involves personal data, including collecting, recording, retrieving, consulting, holding, disclosing or using it; also doing work on the data such as organising, adapting, changing, erasing or destroying it. Personal data be processed fairly and lawfully so data controllers have to meet certain conditions. A data subject must be told the identity of the data controller and why his or her personal information is being or will be processed

Personal data - is that which relates directly to an individual e.g. name, address, date of birth, bank details, HR or medical records, etc. As well as information on staff the organisation will hold a range of personal information relating to Trustees, Donors, Friends Organizations, Marketing and Business contacts etc. which will receive equal protection.

Sensitive information – data relating to a person's

- racial or ethnic origin
- political opinions
- religious or other beliefs of a similar nature
- trade union memberships
- physical or mental health or condition
- offences (including alleged offences)
- criminal proceedings, outcomes and sentences.

5.0 Disclosure of Personal Information

Strict conditions apply to the passing of personal information both internally and externally. The right to confidentiality should be respected where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available provided there is:

- a legal obligation to do so; or
- the information is clearly not intrusive in nature; or
- the member of staff has consented to the disclosure; or
- the information is in a form that does not identify individuals.

6.0 Procedures for the Handling of Personal Information

The National Museums NI will, through appropriate management procedures and controls:

- fully observe conditions regarding the fair collection and use of personal information;
- meet its legal obligations to specify the purposes for which personal information is used;
- collect and process appropriate personal information, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of personal information used;
- apply strict checks to determine the length of time personal information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the legislation;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside the European Economic Area without adequate safeguards.

In addition, National Museums NI will ensure that:

- responsibility for data protection in the organisation is assigned to a specific member of staff; [see Appendix A]
- everyone managing and handling personal information understands that they are directly and personally responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made every three years of the way personal information is managed, staff responsible for this audit are identified in Appendix A;
- methods of handling personal information are regularly assessed and evaluated.

7.0 Staff Responsibilities

All staff have responsibility for the protection of personal data and will be made fully aware of these procedures and of their duties under the legislation.

Data Protection legislation applies not only to National Museums NI as an organisation, but also to all individual staff who work within it. Personal data used by staff while performing their various business functions, must at all times be securely stored.

Personal information held by National Museums NI may be recorded:

- as part of a major computer system
- as a document on a PC or laptop
- as letters or other documents and stored in a card index or box file for example
- as part of an email or an attachment

The various main computer systems e.g. Payroll, HR, Email etc will all have inbuilt security whereby users must be set up with a username and password in order to gain access.
For further information please see the ICT Security Policy.

- Staff will log on to these systems using only their own name and password
- Staff will not give their password to anyone else.
- Personal Information held in hard copy form will be afforded adequate protection and will be kept in locked cabinets when not in use, (contact the Data Protection Officer for advice in relation to security of hard copy files).

Information recorded by staff during the various service processes will be appropriately securely managed from the time it arrives through the cycle right up to the point where it is obsolete and is deleted from a computer system or removed from paper records archive storage for secure disposal.

Whenever data is taken outside the confines of its home building the following guidelines will be followed:

- Personal information in word documents or spreadsheets will be password protected.
- Laptops will always be stored securely
- Personal information will only remain on the laptop as long as is necessary
- Memory sticks will be password protected if they contain sensitive data.
- Personal information will only be taken outside the Museum when absolutely necessary and never without the express permission of the line manager.
- Any incident where data is lost/stolen or even misplaced will be reported immediately to the Head of Department and to the Data Protection Officer
- Any third parties who are users of personal information supplied by National Museums will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the Museum

The process to be followed for reporting any Data Protection breaches is outlined in Appendix B.

8.0 Access to Personal information

Anyone who has personal information managed by National Museums NI has a right of access to that information. This is known as a subject access request. The request should be in writing to the Data Protection Officer, providing their name, contact details and the nature of the request. A Subject Access Request form is provided in appendix D. Individuals may be asked to provide a form of identification prior to any information being released. This is to ensure that personal information is only released to the person the information is about. Information will be provided within 30 days of receipt of a written request for access.

A request may be received for information which is not personal to the enquirer. In such a case, the enquirer should be informed that the information sought cannot be released to him/her under data protection legislation. It may, however, be appropriate to consider the request under the Freedom of Information (FOI) Act 2000. Further details about the FOI Act can be obtained from the Data Protection Officer.

Should any individual be dissatisfied with how their request to access personal information has been dealt with they may request a review that a review be undertaken. Any such request for a review should be addressed to the National Museums NI Chief Operating Officer.

9.0 Fees

The data protection legislation provides that up to £10 may be charged as a fee for providing information to a data subject. At present it is not National Museums NI's policy to make a charge for the provision of information in response to requests received.

10.0 Implementation

In National Museums NI, responsibility for ensuring compliance with data protection legislation rests with the Chief Operating Officer, the Data Protection Officer and the Head of OD&HR [see Appendix A]. The Data Protection Officer must be informed of all subject access requests and will provide help and advice in dealing with cases. He/she will also have overall responsibility for:

- the provision of data protection training for staff;
- the development of best practice guidelines;
- carrying out compliance checks to ensure adherence, throughout the organisation National Museums, with data protection legislation.

National Museums NI currently has a number of purposes (i.e. purposes for which personal data held by it are being processed) registered with the ICO which can be inspected on his website under "Register of Data". The organisation's registration number is Z6753239. The Data Protection Officer must continue to notify the ICO of any significant changes which would affect our current registration, whether this consists of new databases being used, existing ones no longer being maintained, or amendments to the purposes for which current ones are registered. As the ICO only wishes to know in broad terms of our data holdings, it

will not be informed automatically of every individual dataset. If in doubt, the Data Protection Officer should be consulted on any changes.

11.0 Awareness of Data Protection Regulations

Staff and any relevant third parties will be advised of these procedures which will be posted on National Museums NI's internet and intranet sites, as will any subsequent revisions. All staff and relevant third parties are to be familiar with and comply with the procedures at all times.

Any queries about data protection in National Museums NI should be addressed to the Data Protection Officer. Further information can also be found on the ICO's website at www.ico.org.uk

The contacts for data protection related matters in National Museums NI are identified in Appendix A.

The process to be followed for reporting any data breaches is outlined in Appendix B.

A summary of the requirements of the General Data Protection Regulation is outlined in Appendix C.

Appendix A

The Data Protection contact within National Museums NI can be contacted as follows:

Data Protection Officer
gdpr@nationalmuseumsni.org
National Museums Northern Ireland
Tel: 02890 428428

Appendix B

Reporting Data Protection Breaches

National Museums NI will make every effort to avoid breaches of data protection legislation and in particular the loss of personal data. However, it is possible that mistakes will occur on occasion. What is important in these circumstances is that the organisation responds appropriately.

Data breaches could include, for example, loss or unintentional disclosure of personal data relating to staff or public- whether that is on portable media, via email or through the loss of a paper file or files. Even the loss of data relating to one individual would be of concern, especially if the data related to sensitive matters such as financial or disciplinary matters.

It is important that members of staff know what to do if they become aware of a data breach. The Information Commissioner has the power to fine authorities up to £17m and a higher fine is likely if an initial breach is not handled appropriately. The following steps should be taken in the event of a data breach.

1. Any member of staff who becomes aware that they or another person has caused, or may have caused, an unintentional disclosure of personal data held by National Museums NI, or some other breach of the data protection legislation, is responsible for reporting it at the earliest possible point.

2. The breach should be reported to their line Manager and via email to the Data Protection Officer at gdpr@nationalmuseumsni.org and to the Head of HR & OD at hr@nmni.com with the subject line "Data breach report – urgent". The email should indicate:
    - the data affected;
    - how many individuals' records have been disclosed/are affected;
    - the current situation – has the breach been contained and if not, how many people have access to the affected data;
    - what action has been taken to resolve the breach;
    - how the breach happened;
    - when this breach occurred/began;
    - whether there have been similar occurrences previously;
    - any other details that are thought relevant.

3. The Data Protection Officer (or the Head of HR & OD in his absence) will investigate the breach. They will talk to the person responsible for the data affected and their line manager to ensure that they are aware of the breach and are taking necessary action. The incident will also be reported to the Chief Operating Officer.

4. The Data Protection Officer (or Head of HR & OD) will consider how serious the breach is, with due regard to current guidance from the Information Commissioner. The factors they will consider will be:
    - potential harm to data subjects (e.g. possibility of identity theft or other fraud/theft);
    - volume of data disclosed (i.e. number of individual data subjects affected);
    - sensitivity of the data.

5. If the Data Protection Officer, Head of HR & OD and Chief Operating Officer consider a breach to be serious enough, bearing in mind these factors, the Chief Executive will be informed and kept up-to-date with developments.

6. If the Data Protection Officer, Head of HR & OD and Chief Operating Officer consider a breach to be serious enough, with regard to current guidance from the Information Commissioner's Office, they will after consulting the Chief Executive inform the Information Commissioner's Office and the Sponsor Department of the breach (see ICO Guidance on Security Breach Management.

    This must be done within 72 hours of the breach having been identified.

7. If the breach is reported to the Information Commissioner's Office, or the data breach is likely to come to the attention of the media, the Data Protection Officer or the Head of HR & OD will inform the Director of Public Engagement.

8. With regard to current Information Commissioner's Office guidance, the Data Protection Officer or Head of HR & OD will consider whether it is appropriate to contact the data subjects affected to inform them of the breach, and if so, how best to conduct this (e.g. letter, email, press release).

9. In the case of identity theft or other fraud the Chief Operating Officer will consider the need to liaise with the PSNI and the relevant financial institutions. (Please see DAO DFP 12/07 for further guidance in these circumstances).

10. The Data Protection Officer or Head of HR & OD will make recommendations to the person responsible for the data concerned to ensure that the breach is not repeated. It will be the responsibility of that person to ensure that the recommendations are put in place and that they update the Data Protection Officer on progress with implementation. The Data Protection Officer will ensure that any learning outcomes of the breach are communicated to all appropriate staff.

11. In the case of serious breaches, the Chief Executive will submit a report to the Board of Trustees.

Appendix C

General Data Protection Regulations

From 25 May 2018 the General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998, which was brought into law as a way to implement the 1995 EU Data Protection Directive. GDPR seeks to give people more control over how organisations use their data. It also ensures data protection law is almost identical across the EU.

In the full text of GDPR there are 99 articles setting out the rights of individuals and obligations placed on organisations covered by the regulation. These include allowing people to have easier access to the data organisations hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people they collect information about. National Museums NI will take the following steps to ensure compliance with the directive.

1) Lawful, fair and transparent processing

- We will ensure that all processing of personal data is based on a legitimate purpose.
- We will not process data for any purpose other than the legitimate purposes.
- We will inform data subjects about the processing activities on their personal data.

2) Limitation of purpose, data and storage

- We will not process personal data outside the legitimate purpose for which the personal data was collected
- We will ensure that no personal data, other than what is necessary, be requested
- We will ensure that personal data is deleted once the legitimate purpose for which it was collected is fulfilled

3) Data subject rights

- The data subjects have been assigned the right to ask the organisation what information it has about them, and what the company does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data. We will respond to Data Subject requests within 30 working days.

4) Consent

- As and when National Museums NI has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent will be asked from the data subject. Once collected, this consent will be documented, and the data subject will be allowed to withdraw their consent at any time.
- For the processing of children's data, explicit consent of the parents (or guardian) if the child's age is under 16 will be sought.

5) Personal data breaches

- We will maintain a Personal Data Breach Register and, based on severity, the regulator and data subject will be informed within 72 hours of identifying the breach.

6) Privacy by Design

- We will incorporate organisational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects will be ensured by default.

7) Data Protection Impact Assessment

- To estimate the impact of changes or new actions, a Data Protection Impact Assessment (DPIA) will be conducted when initiating a new project, change, or product. The DPIA procedure will be carried out when a significant change is introduced in the processing of personal data. This change could be a new process, or a change to an existing process that alters the way personal data is being processed.

8) Data transfers

- We will ensure the protection and privacy of personal data when that data is being transferred outside the company, to a third party and / or other entity within National Museums NI.

9) Data Protection Officer

- The Data Protection Officer will have the responsibility of advising National Museums NI about compliance with GDPR requirements.

10) Awareness and training

- We will create awareness among employees about key GDPR requirements, and conduct regular training to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible.

Appendix D

National Museums NI
Subject Access Request Form

1. Details of person requesting information

Name	
Address	
Tel.	
Email	

2. Are you the data subject? Yes /No *(delete as appropriate)*

If **Yes**: Proof of identity will be required before any information can be released to you. This should include something bearing your signature, *e.g.* your driving licence or passport. Copies will be accepted.

If **No**: You will need to provide written authority from the data subject on whose behalf you are making the request. (Please answer question **3**.)

3. Details of data subject if different from above

Name	
Address	
Tel.	
Email	
Relationship of requestor to data subject	

4. Describe the information you require. Please provide as much relevant detail as possible.

5. Declaration

I, …….. (*your name*), certify that the information provided on this form is true and accurate. I understand that National Museums Northern Ireland will need to confirm my/the data subject's identity, and more detailed information may be required in order to locate the required personal data.

Signature:

Date:

Please return this form to the Data Protection Officer by post to:

- National Museums NI
  153 Bangor Road
  Cultra
  BT18 0EU

- Make sure you have enclosed:
  - proof of your identity
  - proof of the data subject's identity (if different from requestor)
  - written authorisation to act on the data subject's behalf (if applicable)
  - stamped addressed envelope to return original proof of identity/written authority documents

National Museums NI will process your data collected from this form in accordance with data protection legislation. This information will only be used to handle your request and will not be kept any longer than necessary.