NATIONAL MUSEUMS NI

Data Protection Policy

December 2024

DOCUMENT INFORMATION AND VERSION CONTROL

Version Control			
Version	**Reviewed By**	**Date of Review**	**Summary of Changes**
1	Senior Management	4/12/24	
2	Audit & Risk Assurance Committee	10/12/24	
3	Board of Trustees	N/A	

Policy Last Updated: November 2021

Table of Contents

1. Purpose of Policy 4
2. Applicable Legislation 4
3. Procedure owner / Contact 4
4. General Data Protection Regulation in the UK ('UK GDPR') 4
5. Purpose of Policy 5
6. The Data Protection Principles 5
6.1. Personal data shall be processed fairly and lawfully and, in particular, shall not be 5
6.2. 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. 6
6.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. 6
6.4. Personal data shall be accurate and, where necessary, kept up to date. 6
6.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6
6.6. Personal data shall be processed in accordance with the rights of data subjects under the legislation. 6
6.7. 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. 6
6.8. Personal data shall not be transferred to a country or territory outside the UK or 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. 6
7. Definitions 6
8. Disclosure of Personal Information 7
9. Procedures for the Handling of Personal Information 7
10. Staff Responsibilities 8
11. Access to Personal information 9
12. Fees 10
13. Implementation 10
14. Awareness of Data Protection Regulations 11
15. Appendix A 12
16. Appendix B 12
17. Appendix C - Links to Regulations and Other Useful Guidance & Resources 14

1. Purpose of Policy

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. Applicable Legislation

- Data Protection Act 2018 ("UK GDPR")
- Information Commissioners Office – guidance documents

3. Procedure owner / Contact

James Lewsley
Data Protection Officer
Email: gdpr@nationalmuseumsni.org

David Milnes
Information Officer
Email: gdpr@nationalmuseumsni.org

4. General Data Protection Regulation in the UK ('UK GDPR')

The Data Protection Act 2018 is the United Kingdom's implementation of the (EU) General Data Protection Regulation (GDPR).

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

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

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

5. Purpose of Policy

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, donors, trustees and users of our services to allow us to monitor performance, achievements, operational issues, management of the collections 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, our stakeholder, 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 UK GDPR.

6. The Data Protection Principles

6.1. 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

6.2. 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.

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

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

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

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

6.7. 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.

6.8. Personal data shall not be transferred to a country or territory outside the UK or 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.

7. 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.

8. 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.

9. 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 UK or 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 senior members 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.

10. 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 IT systems will all have inbuilt security whereby users must be set up with a username and password in order to gain access.

- 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 Information Officer for advice in relation to security of hard copy files).

For further information please refer to the ICT Security Policy.

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 your Head of Department, the ICT Manager and 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.

11. 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 C. 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 Colin Catney, Chief Operating Officer.

12. Fees

The data protection legislation provides that A public authority can charge a disbursement for the cost of processing and sending the information to a data subject, such as photocopying and postage information. At present it is not National Museums NI's policy to make a charge disbursement for requests received.

However, if National Museums NI Determines that complying with a request would cost more than £450, then the request can be refused or alternatively the full cost sought from the requestor.

13. Implementation

In National Museums NI, responsibility for ensuring compliance with data protection legislation rests with the Chief Operating Officer and the Data Protection Officer. 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, 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 **ZB663671**. 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.

14. 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 Trustees, Staff and relevant partners 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 Information Officer in the first instance. 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.

Links to the General Data Protection Regulations and other useful information is outlined in Appendix C.

15. Appendix A

Data Protection contacts within National Museums NI are;

James Lewsley
Data Protection Officer
Email: gdpr@nationalmuseumsni.org

David Milnes
Information Officer
Email: gdpr@nationalmuseumsni.org

16. 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 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 Information Officer in his absence) will log the incident on the data breach register and investigate the breach. They will engage with the person responsible for the affected data, and their line manager, to ensure that they are aware of the breach and are taking necessary action. The incident should also be reported to the ICT manager, particularly where it relates to the exposure of data privacy due to the loss of equipment such as laptops, tablets, mobile devices etc. Please report all suspected breaches to helpdesk (at) nationalmuseumsni.org

4. The Data Protection Officer 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, 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, 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 will inform the Director of Public Engagement.

8. With regard to current Information Commissioner's Office guidance, the Data Protection Officer 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 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.

17. Appendix C - Links to Regulations and Other Useful Guidance & Resources

- Data Protection Act 2018
- ICO

Corporate Links:

- National Museums NI Website Link
- Privacy Statement