



THE
NATIONAL
MUSEUM



NMRN
Data Protection Policy (GDPR)
June 2018

Version 1.0

Classification Internal

Document Control

Organisation	The National Museum of the Royal Navy (NMRN)
Author	Ethan Fleming – Governance Manager
Owner	Governance Manager
Subject	Data Protection Policy
Review date	01/06/2019

Revision History

Revision Date	Version Number	Revised By	Description of Revision
01/06/2018	1.0	Ethan Fleming	Document created

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Executive Director Resources	Sarah Dennis	5/6/18
	Audit and Governance Committee	13/6/18

Document Distribution

This document will be distributed to:

Name	Email Address / Location
All Staff and Volunteers	NMRN HQ (Staff Room)
All Staff and Volunteers	Explosion (Staff Room)
All Staff and Volunteers	FAAM (Staff Room)
All Staff and Volunteers	RNSM (Staff Room)
All Staff and Volunteers	RMM (Staff Room)
All Staff and Volunteers	HMS Caroline (Staff Room)
All Staff and Volunteers	NMRN Hartlepool (Staff Room)
Trustees and Committee Members	Email
Stakeholders	Workplace

Table of Contents

1.0	Policy Statement	3
2.0	Purpose	3
3.0	Scope.....	3
4.0	Definition	3
5.0	Policy Compliance	8
6.0	Review and Revision	8

1.0 Policy Statement

It is the responsibility of all that handle or come into contact with personal data to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

2.0 Purpose

This policy aims to ensure:

- Compliance with the General Data Protection Regulation and the upcoming Data Protection Act 2018

3.0 Scope

This policy applies to all NMRN staff, volunteers, and casual members of staff, trustees, committee members and contractors.

4.0 Definition

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5.0 Principles

Principle A Lawfulness, fairness and transparency

All personal data will only be retained or processed under a documented legal basis (see Appendix A), any adverse effects on a data subject from the processing will be considered and documented with any adverse impacts mitigated and with justifiable reasons to continue the processing. Data will only be used in a manner in which a reasonable person would expect it to be used and in the rare occasion that this is not so this will be clearly documented and justified. When collecting data we will be as open and honest as possible and not seek to mislead or confuse data subjects. Personal data will not be used in the transgression of data protection laws or any other UK and international laws.

Principle B Purpose Limitation

Personal data will have a documented purpose/purposes for processing which we will notify individuals of. These purposes will be kept under regular review and any documentation or privacy notices updated accordingly as required. NMRN will use data for the purpose provided and if it requires the data for any other purposes an assessment will be undertaken to determine if this is compatible with the original purpose or if specific consent is required from the individuals involved to allow the new processing. Data may be processed for the following reasons without seeking consent as defined in GDPR as compatible:

- Archiving purposes in the public interest;
- Scientific or historical research purposes; and
- Statistical purposes.

Principle C Data minimisation

Once purposes have been identified for data processing, data collected will be adequate, relevant and necessary to the data processing identified. Data will be regularly reviewed to ensure that only data that is required for the purposes is held. Data subjects retain the right to complete any data which is inadequate for the purposes identified or request the erasure of any excessive data. Requests will be fulfilled as promptly as possible within a maximum of one month.

Principle D Accuracy

NMRN will take all reasonable steps to ensure that data collected is accurate which may include carrying out due diligence exercises to determine accuracy. The source of data will be appropriately recorded. Where needed processes will be in place to ensure data is kept up to date to continue to allow processing, if required for audit purposes or to show compliance a record of any mistake will be kept and clearly identified and retained in line with the retention of the corrected data.

NMRN recognises the right of data subjects to challenge the accuracy of data held and update or delete it with their requirements if it is appropriate. Records of successful and unsuccessful challenges to this will be retained in line with the retention of the data it concerns.

Principle E Storage Limitation

Data will only be retained for as long as required with retention requirements outlined in the NMRN Data retention guidelines available on Workplace and the Snap Drive. After this time data will be anonymised to be retained indefinitely or erased unless it is required for the following exemptions:

- Archiving purposes in the public interest;
- Scientific or historical research purposes; and
- Statistical purposes.

The proper disposal of data is important to minimise the risk of data breaches, to comply with legislation and deliver business efficiencies. Further details on the proper disposal of electronic hardware may be found in the IT Disposal and Destruction policy available on Workplace and the S Drive. Paper files should be disposed of securely by shredding.

Principle F Integrity and confidentiality (Security)

The safeguarding of data and processing is important to the NMRN and all appropriate technical and organisational measures to ensure data security will be undertaken. Risks will be assessed for processing activities to determine to security measures to be undertaken along with a consideration of cost and reasonable steps to be undertaken. This will include ensuring that the appropriate back up facilities are in place to restore data if required. IT security controls are regularly tested with the appropriate software and third party providers, with alerts in place for infringements. Where possible encryption will be implemented.

An Information Security Policy is in place and may be found on Workplace and the S Drive. This and other appropriate policies are reviewed once a year as a minimum by the Head of IT.

Accountability

NMRN will seek to show full accountability with GDPR with a range of appropriate policies and documentation of processing activities. Accountability will be demonstrated with the appropriate security measures and reporting any breaches of personal data in line with the Data Breach Policy. Data Privacy Impact Assessments will be undertaken for projects that include the processing of personal data particularly when this is high risk. All accountability policies and documentation will be reviewed at least yearly.

Contracts with data processors will include the appropriate clauses to require accountability by third parties to be supplied and to indemnify NMRN on failings of any third parties.

NMRN has chosen not to appoint a Data Protection Officer, as approved by the Audit and Governance committee on 13th June 2018. The Executive Director of Resources is the Data Protection Lead for the organisation with responsibility for reporting to the Audit and Governance Committee and the appropriate boards.

6.0 Rights

Right to Be Informed

NMRN will provide the following details to individuals:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

This will be provided in a number of appropriate forms where possible and will use clear language to explain an individual's rights. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests.

Right to Access

A subject access request policy is in place and is available via Workplace or the S Drive, NMRN is committed to responding to requests within one month. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests.

Right of Rectification

NMRN recognises that data subjects have the right to rectify erroneous data and is committed to responding to written or verbal requests to this within one month. NMRN is also committed to rectifying data with any third party processors within one month. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests. A record of successful and non-successful requests will be retained with the data.

Right to Erasure

All data subjects retain a right of erasure (right to be forgotten) in certain circumstances as follows:

- The personal data is no longer necessary for the purpose which it was originally collected or processed it for;
- Consent is the lawful basis for holding the data, and the individual withdraws their consent;
- When legitimate interests is being relied on as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- Processing of the personal data for direct marketing purposes and the individual objects to that processing;
- Data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- To comply with a legal obligation.

Requests may be made in writing or verbally and NMRN is committed to undertaking to erase the data within one month or respond with that this is not possible with reasons explained. Any disputes will be retained with the original data. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests.

Right to Restrict Processing

Data subject have the right to request the restriction or suppression of processing for the following causes:

- The individual contests the accuracy of their personal data and NMRN is verifying the accuracy of the data;

- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- Data is no longer needed but the individual needs NMRN to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to NMRN processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

This will include the restriction on third party processors to NMRN. NMRN is committed to responding to requests within one month, explaining if the restriction has taken effect or not and explaining reasons why not. NMRN will take the appropriate steps to restrict processing by removing data from systems or making it unavailable to staff. A record of successful and non-successful requests will be retained with the data. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests.

Right to Data Portability

NMRN recognises that data subjects have a right to data portability to allow them to obtain and reuse their data elsewhere for different services. NMRN is committed to a reasonable approach to providing this data recognising that maintaining IT systems compatible with all other IT systems is not always possible. Data will be provided in a structured, commonly used, machine readable manner with the most common manner likely to be a CSV file. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests. Requests will be responded to within one month.

Right to Object

NMRN recognises a data subjects right to object to processing and the different circumstances this can take place. NMRN will treat each objection subjectively and is committed to responding within one month. If requests are manifestly unfounded, incorrect or excessive NMRN reserves the right to charge or not comply with any requests. Requests will be responded to within one month.

Rights related to automated decision making including profiling

NMRN will only undertake automated decision making in the following circumstances:

- Necessary for the entry into or performance of a contract; or
- Authorised by Union or Member state law applicable to the controller; or
- Based on the individual's explicit consent.

If this style of decision making is undertaken decisions to automate it will be documented and will be reviewed at least once a year or more often as business requires. Information will also be provided to the data subjects including allowing them to request human intervention.

7.0 International Transfers

As part of standard business NMRN will not seek to transfer data out of the EU or any of the bodies that make up the EU. If business needs require this then a review to ensure adequate safeguards are in place will be undertaken.

8.0 Policy Compliance

All users with access to personal data must comply with this policy. This includes staff, volunteers, trustees and third party contractors. Suppliers who manage IT equipment on behalf of the NMRN must also comply with this policy.

9.0 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Governance Manager.

END OF DOCUMENT

Data Protection Policy