The Merchant Navy Association

Registered as a charity in England & Wales Number 1135661

DATA PROTECTION POLICY STATEMENT

Policy, scope and objectives

1. **United Kingdom's General Data Protection Regulations (UK-GDPR)** are enshrined in the **Data Protection Act 2018 – updated on 1st January 2021**. The Council of the Merchant Navy Association (MNA) are committed to compliance with all relevant UK laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information MNA holds in accordance with the UK-GDPR.

2. **Objectives** The MNA is a Registered Charity No 1135661 based in the United Kingdom and founded in 1989 to:
   - Foster comradeship and consideration to all those in the community of the sea
   - Endeavour to assist members and, when appropriate, other eligible persons to find access to information and practical support on such matters as pensions, health, social security, debt management and other subjects affecting their welfare.
   - Endeavour to provide grants to members and other eligible persons in financial need to help with the purchase of goods, services or facilities or, in exceptional circumstances, payment of priority debts.
   - Signpost those seeking advice about a career at sea, to appropriate organisations and encourage both young and life-long learners to maximise their opportunities
   - Put those seeking background and historical information about the Merchant Navy in touch with appropriate sources.

3. **Personal Information Management (PIM)** is defined as the activities people perform to acquire, organise, maintain, retrieve and use personal information items such as documents (paper-based and digital), web pages and email messages for everyday use to complete tasks. The MNA's objectives for the PIMS are that it should:
   - enable it to meet its own requirements for the management of personal information;
   - support organisational objectives and obligations;
   - impose Protections in line with MNA's acceptable level of risk;
   - ensure that MNA meets applicable statutory, regulatory, contractual and/or professional duties;
   - protect the interests of individuals and other key stakeholders.

4. **Protection of Personal Data Policy in Practice** The MNA is committed to complying with data protection legislation and good practice. This includes:
   a) processing personal information only where this is strictly necessary for legitimate organisational purposes;
   b) retaining all personal information securely, accurately and up to date;
   c) collecting only the minimum relevant personal information required for these purposes.
   d) not processing excessive personal information;
   e) providing clear information to individuals about how their personal information will be used and by whom;
   f) processing personal information fairly and lawfully;
   g) maintaining an inventory of the categories of personal information processed by MNA;
   h) retaining personal information only for as long as is necessary for legitimate organisational purposes;
   i) respecting individuals' rights in relation to their personal information, including their right of subject access;
   j) no personal detail will be released to a third party without that individual's express consent.
   k) no personal data revealing the following information will be requested or recorded including:
      - racial or ethnic origin;
      - political views;
      - religious or philosophical beliefs;
      - trade-union membership;
      - genetic and biometric data;
      - data concerning health;
      - data concerning a person's sex life or sexual orientation.

   l) membership lists will only be available to delegated members of the Executive Committee.

m) hard copies of all personal data such a membership will be kept in a secure filing system.
n) computer-based records of all personal data will be password protected.
o) any person wishing to see records held about them may request this in writing and that information shall be forwarded to them, either by post, or email to their registered address within 21 days.
p) any member, or other person, may request reasonable amendments to any data within 21 days.
q) any person may request the removal of all information held about them, but must understand that this is likely to terminate their membership.
r) when a member resigns, unless otherwise requested, their details will be securely retained for up to two years in case they wish to be reinstated.
s) in the event that a member dies, unless otherwise requested by their next of kin, only their name will be retained in the records. This will allow the MNA to answer any enquiries concerning that person's wellbeing.
t) all paper obsolete based records will be properly shredded and disposed of.
u) all obsolete computer-based records will be permanently deleted.

1.5 Complaints

Data Subjects who wish to complain to the MNA about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer, in writing, via the National Secretary or by email to chairman@mna.org.uk.

Data subjects may also complain directly to the Independent Commissioners Office (ICO)

Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer.

NOTES

Notifying the Information Commissioner The MNA has notified the Information Commissioner that it is a data Protectioner and that it processes certain information about data subjects. MNA has identified all the personal data that it processes, and this is contained in a Data Inventory Register

The Data Protection Officer is responsible for reviewing the details of notification, in the light of any changes to MNA's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments.

The policy applies to all Council members and interested parties of MNA. Any breach of the UK-GDPR or this PIMS will be dealt with by the Council. If it is construed to be, potentially, a criminal offence, the matter will be reported as soon as possible to the appropriate authorities.

Background to the General Data Protection Regulation (UK-GDPR)

The UK -GDPR's purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Data Protection Officer (DPO)– is the person, nominated as such by the MNA's Council.

Residence of the DPO – the main residence of the registered DPO will be the place in which he, or she, makes decisions as to the purpose of its data processing activities.

Data subject – any individual who is the subject of personal data held by an organisation.

Data subject consent - means any information freely given by the *Data subject*. For example, this will include contact details of members, or those applying for membership.

Data Processing – any operation, or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, dissemination and deletion of records.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the Protectioner to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child – the UK-GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, DPO, data processor and persons who, under the direct authority of the DPO, are authorised to process personal data.

Filing system – any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Risk Assessment

To ensure that MNA is aware of any risks associated with the processing of types of personal information and regularly reviews its risks.

MNA has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of MNA. MNA shall manage any risks which are identified by the risk assessment to reduce the likelihood of a non-conformance with this policy.

Data protection principles

All processing of personal data must be done in accordance with data protection principles of the Regulation, and MNA's policies and procedures are designed to ensure compliance with them.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them. To

- make requests regarding the nature of information held and to whom it has been disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of automated decision-taking process that will significantly affect them.
- sue for compensation if they suffer damage by any contravention of the UK-GDPR.
- take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- request the ICO to assess whether any provision of the UK-GDPR has been contravened.
- have the right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another DPO
- object to any automated profiling without consent.

Data subjects may make data access requests. This procedure also describes how the MNA will ensure that its response to the data access request complies with the requirements of the Regulation.

Consent

MNA understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

MNA further understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or because of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

The MNA should avoid becoming involved in any matters that involve children under the age of 16. In the very unlikely event that it does so, parental, or custodial authorisation must be obtained.

Security of data

All Council members are responsible for ensuring that any personal data which the MNA holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the MNA to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it:

- Paper based records must be stored in a secure drawer or filing cabinet;
- Computerised records must be password protected

Care must be taken to ensure that PC screens and terminals are only visible to authorised personnel. All Council members are required to read and have understood this Policy before they are given access to organisational information of any sort.

Paper based records may not be left where they can be accessed by unauthorised personnel and may not be removed from without explicit authorisation.

Personal data must be deleted, or disposed of, in line with the Data Retention Procedure. Manual records that have reached the end of their retention date are to be shredded and disposed of. Computer based records are to be deleted and then removed from the "recycle bin".

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held the MNA in electronic format and manual records which form part of a relevant filing system. This includes the right of access to confidential personal information obtained from third-party organisations about that person.

Disclosure of data

MNA must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Council members, or others, with access

to records should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the MNA's business.

The UK-GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax;
- discharge of regulatory functions;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member has left the MNA, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. MNA's data retention and data disposal procedures will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

Reviewing the MNA Data Protection Policy

The DPO is responsible for reviewing this policy every 12 months, or when there are any changes in legislation, or in the MNA's working practices that might affect this Policy. The Officer will also be responsible for advising the Council about any proposed changes to the Policy.

This policy was approved by the Council on 24th April 2021.

Signature: Date:

Data Protection Officer