ROYAL NAVAL AMATEUR RADIO SOCIETY

GDPR POLICY

This policy document contains the Royal Naval Amateur Radio Society's General Data Protection Regulation (GDPR) Policy as required by law from 25th May 2018.

5th April 2018

Royal Naval Amateur Radio Society ("the Society")

GDPR POLICY

1. Policy, Scope and Objectives

1.1 The Committee generally located at Building 512, HMS Collingwood, Fareham, PO14 1AS is committed to comply with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information the Society collects in accordance with the General Data Protection Regulation (GDPR). The Society has developed, implemented, maintains and continuously improves upon a documented personal information management system (PIMS).

1.2 Scope

The scope of the PIMS considers the organisational structure, management responsibility, jurisdiction and geography.

1.3 Objectives of the PIMS

The Society's objectives for the PIMS is to enable the Society to meet its own requirements for the management of personal information;

that it should support organisational objectives and obligations,
that it should impose controls in line with the Society's acceptable level of risk,
that it should ensure that the Society meets applicable statutory, regulatory, contractual and/or professional duties,
that it protects the interests of individuals and other key stakeholders.

The Society is committed to complying with data protection legislation and good practice including:

a) Processing personal information only where this is strictly necessary for legitimate organisational purposes
b) Collecting only the minimum personal information required for these purposes and not processing excessive personal information
c) Providing clear information to individuals about how their personal information will be used and by whom
d) Only processing relevant and adequate personal information
e) Processing personal information fairly and lawfully
f) Maintaining an inventory of the categories of personal information processed by the Society
g) Keeping personal information accurate and, where necessary, up to date
h) Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
i) Respecting individuals' rights in relation to their personal information, including their right of subject access

j) Keeping all personal information secure
k) Only transferring personal information outside the EU in circumstances where it can be adequately protected
l) The application of the various exemptions allowable by data protection legislation
m) Developing and implementing a PIMS to enable the policy to be implemented
n) Where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the Society, and the identification of volunteers/workers with specific responsibility and accountability for the PIMS.

1.4 Notification

The Membership, Website and Commodities Managers are responsible for reviewing the details of notification, in the light of any changes to the Society'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 members and employees of the Society. Any deliberate breach of the GDPR or this PIMS will be dealt with under the Society's disciplinary proceedings and may also be a criminal offence. Should there be a need to report a breach, either of the Membership, Website and Commodities Managers should be notified.

Associates/Affiliates and third parties working with or for the Society, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Society without having first entered into a data confidentiality agreement.

1.5 Background to the General Data Protection Regulation (GDPR)

The GDPR 2016 becomes law on the 25th of May 2018 and replaces the EU Data Protection Directive of 1995 and supercedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its 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.

1.6 Definitions used by the organisation -drawn from the GDPR

Territorial scope

The GDPR will apply to all controllers that are established in the EU who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour to data subjects who are resident in the EU.

Personal Data
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.

Specialised categories of personal data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by the Union or Member State law.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

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, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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 at work, economic situation, location, health, personal preferences, reliability, or behaviour. 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 controller 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.

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

Filing System
Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

2 Responsibilities under the General Data Protection Regulation

Senior Management/the Committee and all those in managerial or supervisory roles throughout the Society are responsible for developing and encouraging good information handling practices within the organisation; responsibilities will be set out in individual job descriptions.

2.1 Management Responsibility of Personal Data

The Membership, Website and Commodities Managers are responsible for the management of personal information within the Society and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

2.1.1 Development and implementation of the PIMS as required by this policy, and;

2.1.2 Security and risk management in relation to compliance with the policy.

2.2 Compliance

Compliance with the data protection legislation is the responsibility of all members of the Society who process personal information.

3 Risk Assessment

3.1 Objective

To ensure that the Society is aware of any risks associated with the processing of particular types of personal information.

3.1.1 The Society has a process for assessing the level of risk to individuals associated with the processing of their personal information.

3.1.2 Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of the Society. The Society shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformity with this policy.

3.2 Data Processes

Where a type of processing in particular, using new technology and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the “rights and freedoms” of natural persons, the Society shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

3.2.1 A single assessment may address a set of similar processing operations that present similar high risks

4 Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the GDPR and the Society’s policies and procedures are designed to ensure compliance with them.

4.1 Personal data must be processed lawfully, fairly and transparently. The GDPR introduces the requirement for transparency whereby information is transparent and easily accessible. The specific information that must be provided to the data subject must, as a minimum include:

4.1.1 The identity and the contact details of the controller and, if any, of the controller’s representative.

4.1.2 The contact details of the Data Protection Officer, where applicable.

4.1.3 The purposes of the processing for which the personal data is intended, as well, as the legal basis for the processing.

4.1.4 The period for which the personal data will be stored.

4.1.5 The existence of the rights to request access, rectification, erasure or to object to the processing.

4.1.6 The categories of personal data concerned.

4.1.7 The recipients or categories of recipients of the personal data, where applicable.

4.1.8 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data.

4.1.9 Any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specified, explicit and legitimate purposes.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing.

4.4 Personal data must be accurate and kept up to date.

4.5 Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.6 The appointed data protection/IT systems lead is responsible for ensuring that all those responsible for processing personal data are trained in the importance of collecting accurate data and maintaining it.

4.7 It is also the responsibility of individuals to ensure that data held by the Society is accurate and up to date.

4.8 Members and employees working on behalf of the Society should notify the Society of any changes in circumstances to enable personal records to be updated accordingly.

4.9 The appointed data protection/IT systems lead is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking in to account the volume of data collected, the speed with which it might change and any other relevant factors.

4.10 On at least an annual basis, the Society will review all the personal data maintained.

4.11 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.12 Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach.

4.13 Personal data must be processed in a manner that ensures its security.

4.14 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

5 Safeguards

An assessment of the adequacy of data protection performed by the data controller should take in to account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination of the information.
- How the information will be used and for how long.
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations.
- The security measures that are to be taken regarding the data in the overseas location.

6 Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance, but for demonstrating that each processing operation complies with the requirements of the GDPR. Specifically, controllers are required to maintain necessary documentation of all processing operations, the implementation of appropriate security measures, perform and record the outcome of Data Processing Impact Assessments (DPIAs), and comply with the requirements for prior notifications.

7 Data Subjects' Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

7.1.1 To make subject access requests regarding the nature of the information held and to whom it has been disclosed.
7.1.2 To prevent processing likely to cause damage or distress.
7.1.3 To prevent processing for purposes of direct marketing.
7.1.4 To be informed about the mechanics of automated decision-making processes that will significantly affect them.
7.1.5 To refuse to have significant decisions that will affect them taken solely by automated processing.
7.1.6 To take action to rectify, block, erase, to be forgotten, destroy inaccurate data.
7.1.7 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 controller.
7.1.8 The right to object to any automated profiling made without consent.

8 Consent

The Society understands “consent” to mean that it has been explicitly and freely given, specific, informed and an unambiguous indication of the data subject’s wishes, which by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to the data subject. The consent of the data subject can be withdrawn at any time.

The Society understands “consent” to mean that the data subject has been fully informed of the intended processing and has signified agreement while in a fit state of mind to do so, and without pressure being exerted upon them.

9 Security of Data

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

Care must be taken to ensure that display screens and terminals are not visible except to authorised members/employees of the Society.

Manual records may not be left where they can be accessed by unauthorised persons and may not be removed from either the Society’s premises or agreed locations without explicit (written) authorisation. As soon as manual records are no longer required for day to day use they must be placed in a secure manual archive or destroyed as appropriate.

10 Rights of Access to Data

Data subjects have the right to access any personal data about them which is held in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by: organisation name, and information obtained from third party organisations about that person.

11 Disclosure of Data

The Society 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 members/employees should exercise caution when asked by a third party to disclose personal data held about another person. It is important to bear in mind whether or not disclosure of the information is relevant to and necessary for the conduct of the Society’s business.

The 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 apprehension or prosecution of offenders.
- Assessment or collection of tax duty
- Discharge of regulatory functions (including health, safety and welfare of persons at work)
- 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 appointed data protection/IT systems lead.