ROYAL AIR FORCES Association
The charity that supports the RAF family

Royal Air Forces Association

Data Protection Policy

Original creation date	December 2015
Version 3.0 creation date	12 Mar 2018
Next review date	1 May 2019
Prepared by	IE Committee
Approved by	Council
Version	3.2

Contents

2. Introduction
3. Policy Statement
4. Registration with the Information Commissioner's Office
5. GDPR Principles
6. Rights of Access by Individuals
7. Roles and Responsibilities
8. Training
9. Breach of Policy
10. Dealing with a Data Breach
11. Associated Data Protection Documentation

Annexes:

A. Glossary of Terms

B. Annual Certificate of Compliance

Enclosures:

1. Privacy Notice

2. Introduction

2.1. The Royal Air Forces Association (the Association) regards the lawful and correct processing of personal data as an integral part of its purpose and vital for maintaining confidence between stakeholders. The Association is committed to valuing the personal information entrusted to it and to respecting that trust by being open and transparent about how it uses, shares and protects personal information. The Association acknowledges that all individuals have the right to expect that appropriate safeguards will be operated to protect the confidentiality and integrity of their personal data or information.

2.2. This policy aims to protect the privacy of and promote the rights of the individuals whose personal and confidential information is held by the Association. The Association will ensure that it has the necessary information to deliver its mission, to manage its employees, membership, beneficiaries and volunteers and to engage with other individuals in delivering its charitable objectives.

3. Policy Statement

3.1. This Data Protection (DP) Policy, together with its supporting Standard Operating Procedures (SOP), is designed to ensure that all activities conducted by the Association safeguard the confidentiality of personal information and comply with the provisions of Data Protection legislation, including the General Data Protection Regulation (EU) 2016/679 ("the GDPR") which comes into force in the UK on 25 May 2018. The GDPR overhauls many areas of the current data protection laws and replaces the UK Data Protection Act 1998 (DPA) and gives individuals more rights and protection regarding how their personal data is used by the Association.

3.2. This DP Policy is applicable to all organisational elements of the Association and to all personnel who are part of or working with the Association including members, volunteers, beneficiaries, employees, customers and suppliers such that all those who have access to any personal data records (see Annex A Glossary of Terms) held by, or on behalf of, the Association, are fully aware of, and abide by, their duties and responsibilities under the GDPR and other data protection legislation (together "Data Protection legislation"). Furthermore, the Association will:

- Ensure all employees and others handling personal data are aware of their obligations and rights under Data Protection legislation and receive adequate data protection training.
- Implement adequate and appropriate physical and technical measures and organisational measures to ensure the security of all data contained in or handled by those systems.
- Where the Association relies on an individual's consent to process personal data it will ensure that consent is specific, informed and freely given. Requests for consent will be clear, prominent and require unambiguous and clear affirmative indication signifying agreement. When requesting consent, the Association will advise individuals of the right to withdraw consent and the Association will not make consent a condition of a contract. The Association will keep records of consent.

- The Association will document what personal data it holds, where it came from and with whom it is shared.
- The Association will provide individuals with all relevant information that they require to understand and exercise their rights under Data Protection legislation and in accordance with this Data Protection Policy. The rights of individuals are set out in the Association Privacy Notice at Enclosure 1, a copy of which is available to users via the Association website at www.rafa.org.uk/privacy.
- The Association will adopt a privacy by design approach to all projects to promote privacy and data protection compliance from the start. At the start of any project and throughout its lifecycle the Association will undertake a Privacy Impact Assessment (PIA), especially for the following:
    - Building new IT systems for storing or accessing personal data;
    - Developing policies or strategies that have privacy implications;
    - Embarking on data share initiative; or
    - Using data for new purposes.
- The Association will only share personal data in accordance with the requirements of Data Protection legislation, taking into account regulatory guidance and will inform individuals of the identity of other parties to whom we may disclose or be required to provide personal data, the circumstances in which this may happen and when any exceptions to this rule may apply.
- Where the Association appoints a third party to process personal data on its behalf, the Association will ensure that the relationship is governed by a binding contracts and that the processor undertakes to process the information only in accordance with documented instructions from the Association, keeping the information secure and confidential.
- Where the Association needs to transfer personal data outside of the European Economic Area (EEA), prior to doing so it will ensure that the party and country to whom the personal data is being transferred can provide the same level of protection as provided by data protection laws in the EEA.

4. Registration with the Information Commissioner's Office

4.1. The Association is registered with the Information Commissioner's Office (ICO) to act as a Data Controller (see Annex A Glossary of Terms) to '*process personal information to enable us to provide a voluntary service for the benefit of the national public as specified in our constitution; administer membership records; to fundraise and promote the interests of the charity; manage our employees and volunteers; maintain our own accounts and records and provide residential care. Our processing also includes the use of CCTV systems for the prevention of crime*.'

4.2. The above registration applies to all Association organisational elements, but where Branch Clubs and Branches additionally handle their own localised personal data, for example Branch Associate membership details, they are to register with the ICO as separate Data Controllers.

5. GDPR Principles

The Association, as Data Controller, is responsible for and will demonstrate accountability for compliance with GDPR. All personnel involved with the Association must only handle personal data in accordance with the following principles as defined in the GDPR:

- **Principle 1:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- **Principle 2:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Principle 3:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle 4:** Personal data shall be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Principle 5:** Personal data will be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.
- **Principle 6:** Personal data shall be in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Rights of Access by Individuals

6.1. Data Protection legislation gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual records held in a structured file, subject to certain exemptions. This is called a Subject Access Request (SAR). DP SOP 001 - Dealing with a Personal Data Subject Access Request (SAR), describes the procedures to be followed within the Association.

6.2. The Privacy Notice at Enclosure 1 describes how Data Subjects may identify that their data is being held or processed. The individual's consent is required before the sensitive personal data (or special categories of data) can be processed by the Association.

7. Roles and Responsibilities

7.1. Council (the Association's Board of Trustees) is ultimately responsible for ensuring the Association meets its legal obligations including in relation to data protection and is responsible for approving this policy.

7.2. The Secretary General, though the Senior Management Team (SMT), is responsible for ensuring this policy is appropriately implemented across the Association and is embedded into Association culture.

7.3. Association managers are responsible for ensuring compliance with this policy in their respective areas of responsibility.

7.4. Everyone viewing, managing or processing personal data at the Association is required to follow this DP Policy and its associated SOPs. Employees are to sign the certificate at Annex B annually.

7.5. The Association is only able to share personal or sensitive personal data with volunteers and with Branch and Branch Club officials who have received, read and agree to use such data in compliance with this Policy and have signed the certificate at Annex B or signed as a Data Processor on the Branch / Branch Club Annual Return Form 1056. Additional DP support for Branches, Branch Clubs, Branch officials and volunteers is available from Branch Support Officers (BSO), Station Officers (SO) and the Area Welfare teams.

7.6. All Employees, Members, Volunteers (including Branch and Branch Club officials) and Contractors are required to:

- Comply with DP SOP 002 - Handling of Personal Data, in relation to obtaining, using and disclosing personal data and sensitive personal data.
- Comply with DP SOP 003 – Personal Data Retention and Disposal.

7.7. The Association's Data Protection Officer (DPO) is the Director of Governance and Risk whose responsibilities include but are not limited to:

- Ensuring those handling personal data on behalf of the Association are aware of their obligations by producing relevant policy and procedures, auditing the arrangements and ensuring relevant people receive training.
- Providing guidance and advice to all personnel in relation to ensuring the Association's compliance with requirements of Data Protection legislation.
- Advising on, and monitoring, data protection impact assessments.
- Monitoring the Association's compliance with Data Protection legislation and this policy, including carrying out annual audits of the Association's data protection arrangements.
- Being the first point of contact with and liaising with the ICO, including reporting on any breaches of Data Protection legislation to the ICO.
- Managing all SARs and being the Association's main contact for data protection.

8. Training

8.1. The Association will provide data protection training to its employees as part of their initial induction and annually thereafter.

8.2. The Association offers the same online training to all volunteers who handle personal data. Further information on data protection training is available from the Area Office or the Learning and Development Manager at HQ. Alternatively send an email to: data.protection@rafa.org.uk. Further advice can be gained from http://www.ico.gov.uk/

9. Breach of Policy

9.1. In the event that personnel fail to comply with this Policy, the matter may be considered as misconduct and dealt with in accordance with the Association's Disciplinary Policy and Procedure.

9.2. Failure to adhere to any of the provisions of this Policy could mean an individual(s) being investigated by the ICO; deliberate unlawful disclosure of personal data is a criminal offence for which an individual can be personally prosecuted under the Data Protection legislation. Members, volunteers and others with whom Association data has been shared may be personally liable for any breach of Data Protection legislation.

10. Dealing with a Data Breach

10.1. The Association is committed to protecting the personal data it holds but recognises that breaches can occur. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

10.2. If a data breach (see Annex A - Glossary of Terms) is suspected action will be taken in accordance with DP SOP 004 - Data Security Breach Procedures

11. Associated DP Documentation

This Policy should be read in conjunction with the Association Information Environment Security Policy (ICT Security Policy 1.0), and the following DP SOPs:

DP SOP 001 - Dealing with a Personal Data Subject Access Request (SAR)
DP SOP 002 - Handling of Personal Data
DP SOP 003 - Personal Data Retention and Disposal
DP SOP 004 - Data Security Breach Procedures

ANNEX A
GLOSSARY OF TERMS

Consent
Any freely given specific and informed indication of the individual's wishes by which the individual signifies their agreement to personal data relating to them being processed. Failure to respond / object should not be regarded as consent. Consent obtained under duress or on the basis of misleading information is not valid. Consent must be appropriate to the age and capacity of the individual and to the particular circumstances of the case. Consent maybe withdrawn by the individual at any time.

Data Breach
A failure leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data.

Data Controller
A person or legal personality who (either alone or jointly or in common with others) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed.
For Association personal data, the Association is registered with the ICO as the Data Controller. Additionally, if Branches and/or Branch Clubs hold separate localised data in the following categories, they are also Data Controllers in their own right and must register the Branch or Branch Club with the ICO (https://ico.org.uk/registration/new) and inform their Area Office.

- If the Branch maintains membership data such as Branch Associate membership which are not managed centrally by the Association.
- If the Branch handles member, beneficiary, employee or other individuals data for Branch use and where the Association is not involved.
- If the Branch Club employs anyone.

Data Extractor
The person who takes data from data sources like the database, which may then be used for further activity. For example, the Membership Support Officer running a report to pull off a table of contact details of Branch members; or the person using the database to compile and send out a list of labels for letters to be sent out.

Data Processor
In relation to personal data or sensitive personal data, means any person who processes that data on behalf of the Data Controller but it is not employed by them.
Data Processors include Branch Secretaries managing membership renewal lists or labels, mailing houses who the Association pass mailing lists to and external support companies who have access to the Association's data.

Data Record
A data record can be in computerised and/or manual form. It may include such documentation such as: Manually stored paper data such as membership records, beneficiary records, employee records, donor records; Handwritten notes; Letters to and from the Association; Electronic records; Printouts; Photographs; Videos and tape recordings.

Data Subject
An identified or identifiable natural person (individual) who is the subject of personal data or sensitive personal data. An identifiable natural person is a living person who can be identified, directly or indirectly, in particular by reference to an identifier such as 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. This includes an employee, member, beneficiary, donor, supporter or volunteer.

Explicit Consent
This is one of the conditions of processing special categories of personal data and must be absolutely clear and requires the individual to consent to the specific processing, the specific type of data, the purposes of the processing and any sharing.

Personal Data

Personal data is defined as all data processed by the Association relating to any identifiable living individual (Data Subject). Examples of personal identifiable data the Association processes include:

- Name, address, email, phone numbers and other contact information.
- Membership number.
- Date of birth.
- Financial information.
- National Insurance numbers and payroll data.
- Information about an individual's health.
- Photographs, video and audio recordings.

Certain types of personal data are regarded as sensitive and attract additional legal protection and hence require additional handling and storage protection. Sensitive personal data (also known as special categories) is considered to be any data that could identify an individual's:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade Union membership.
- Physical or mental health or condition.
- Sexual life.
- Commission or alleged commission of any offence.
- Involvement with any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings.
- Bank account, National Insurance number, and/or identity details such as passport or driving license numbers, etc.

All data collected from people under the age of 16 (or older if there are concerns about mental capacity) is to be treated as sensitive personal data.

Privacy notice
The oral or written statement that individuals are given when information about them is collected is often called a 'fair processing notice' or a 'privacy notice'. The privacy notice should state the identity of the organisation collecting the data, the purpose for which the information will be used, any relevant information on who the data will be shared with, how long the information will be kept for and the rights of the data subject.

Processing
Means recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially, if you have it, you are processing it.

Subject Access Request (SAR)
A written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 30 calendar days of receipt of the request.

Third Party
In relation to personal data or sensitive personal data, means any person other than the data subject, the Data Controller, or any Data Processor or other person authorised to process data for the Data Controller or Data Processor. For example, the police or HM Revenue & Customs.

ANNEX B

---

1. Annual Certificate of Compliance for the Protection of Personal Data:

I certify that any personal or sensitive personal data received from the Association will only be used in accordance with the RAF Association Personal Data Privacy Policy and associated Standard Operating Procedures.

Name

Position　　　　　　　　　　　　　　　　　　　　　Branch

Email Address

Address

Signature　　　　　　　　　　　　　　　　　　　　Date