RPOAS Data Protection Policy

Last reviewed: July 2026

1. Statement

- This Policy is issued in terms of our Articles of Association, Schedule 1, Section 8 and reflects the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025 ,which together govern the handling of personal data in the United Kingdom.
- The Executive Committee of the Retired Police Officers' Association Scotland (RPOAS) prescribes the adoption of this Data Protection Policy at both National and Branch level.
- The Business Model in operation within RPOAS relies on safe and secure Information and Communication Technology (ICT) and the responsible handling of members' data. Any compromise may cause significant damage to both members' trust and the Association's reputation
- Failure to comply may result in restriction of access to Association business or removal from office/membership.

2. Background

2.1. Advances in ICT have changed the ways in which personal information is collected, stored, and used. RPOAS recognises its duty to handle members' personal data with care, security, and respect.

2.2. All personal data must be held securely, used only for legitimate purposes, and processed in line with members' expectations and the law.

3. Legislation

3.1. From 25 May 2018, the EU General Data Protection Regulation (GDPR) applied, and following the UK's exit from the European Union, the UK GDPR alongside the Data Protection Act 2018 continues to apply. The Data (Use and Access) Act 2025 updates both of the aforesaid.

3.2. There are two roles in data processing:

- **Data Controller** – determines the purpose and means of processing personal data
- **Data Processor** – processes data on behalf of a controller

Both roles carry legal responsibility in the event of a data breach.

4. Lawfulness for Processing Members' Data

4.1. When an individual applies to join, RPOAS collects personal information (such as name, postal address, email address and telephone number) in order to provide membership services.

4.2. Data is processed under the lawful basis of legitimate interests (supporting members' welfare, communication, and representation). Consent will only be sought where required (e.g. sharing information with third parties).

4.3. Communications may include:

- Updates on pensions and benefits
- Notifications of events, meetings, or member welfare issues
- Death notices of former colleagues
- General news about members and the Association

(This list is not exhaustive)

4.4. Data is securely stored for the duration of membership and updated at the member's request. RPOAS acts as **Data Controller** and will never sell or share data with third parties for marketing or sales purposes.

4.5. When membership ends, data will normally be deleted within 3 months, unless required for legal, financial, or historical purposes. Archive data may be retained under the lawful basis of legitimate interests for historical membership records, unless the individual objects.

4.6. RPOAS undertakes to process all personal data securely, protecting it against unauthorised access, loss, or damage, using appropriate technical and organisational measures (e.g. access controls, password protection, encryption).

5. Scope

5.1. Data handling within RPOAS must be transparent, accountable, and proportionate to risk.

5.2. Personal data may be accessed by individuals in the following roles (not exhaustive, subject to audit):

- Branch Officials
- National Executive Officers
- RPOAS Administrator and Deputy
- Web Administrator and Deputy

5.3. **T**hird-party organisations formally engaged by RPOAS to process personal data on its behalf must be subject to appropriate contractual and data protection arrangements, including Data Processing Agreements where required under UK GDPR.

5.4. **Suspicious or unusual access must be reported immediately to the national Secretary or to the national Assistant Secretary** (contact email addresses for both are listed in section 8.6 below)

5.5. Personal data includes

- Name
- Membership or identification number
- Date of birth
- Postal address
- Email address
- Telephone number

5.6. Branches must manage membership data in accordance with UK GDPR and this Policy. Breaches of compliance may result in sanctions.

6. Policy of RPOAS

I. RPOAS adopts the principles of the UK GDPR and commits to rigorous and secure data management across the Association.

II. All new members will provide signed confirmation that they understand how their data will be used, stored, and managed.

III. Data will only be shared with third parties where legally required or with the member's explicit consent.

IV. Local Branch Secretaries will ensure all members are informed of data protection responsibilities and will manage local records in compliance with this Policy.

V. Data management will be reviewed annually. Each Branch must submit a Certificate of Fitness to the National Secretary within 14 days of their AGM. GDPR compliance must be a standing agenda item at Branch AGMs.

Grades of compliance are:

- A. Fully compliant
- B. Partially compliant
- C. Not compliant

VI. Suspected data breaches must be reported immediately to the national Secretary or to the national Assistant Secretary (**contact email addresses for both are listed in section 8.6 below**). Where there is a risk to individuals, the Information Commission (the IC – formerly known as the ICO) will be notified within **72 hours** in accordance with legal obligations.

VII. Members have the following rights under UK GDPR:

- Access to their personal data
- Correction of inaccurate data
- Erasure ("right to be forgotten")
- Restriction of processing
- Objection to processing
- Data portability
- Right to complain to the Information Commission (the IC)

VIII. The Association will maintain and publish a **Privacy Notice**, setting out how members' data is processed, their rights, and how to exercise them.

7. Data Retention and Disposal

7.1. RPOAS holds only limited personal data relating to members, primarily for communication, welfare, and administrative purposes.

7.2. Personal data will be retained only for as long as is necessary to fulfil the purposes for which it was collected, including any legal, accounting, or reporting requirements.

7.3. The following general retention schedule applies:

Data Type	Purpose	Retention Period	Disposal Method
Member contact details (name, address, phone, email)	Membership administration and communication	Held for duration of membership; deleted within 3 months of cessation	Secure deletion or shredding
Membership forms and consent records	Proof of lawful basis and consent	3 years after membership ends	Secure deletion or shredding
Correspondence with members	Administration and welfare contact	2 years after last contact	Secure deletion
Committee/Branch records containing personal data	Operational record keeping	5 years after date of record	Secure deletion
Archived membership lists (for historical record only)	Maintaining an historical record of membership (names only)	Indefinitely	Stored securely, minimal data only

7.4. Branch Secretaries and Officers are responsible for ensuring data is deleted or securely destroyed when no longer required, in line with this schedule.

7.5. Where data is stored electronically, deletion must include the removal of all copies, backups, and email records containing personal information.

7.6. Paper records must be shredded or otherwise securely destroyed.

7.7. The Executive Committee may approve adjustments to this retention schedule if required by law or operational necessity, ensuring members are informed where relevant.

8. Data Storage and Security

8.1. RPOAS and its Branches will ensure all personal data is stored and handled in a manner that maintains its confidentiality, integrity, and availability.

8.2. Personal data will be stored securely, whether in paper or electronic form, with access restricted to authorised office bearers who require it for legitimate Association purposes.

8.3. **Electronic records**

- All devices used to hold or access RPOAS data (including laptops, tablets, and mobile phones) must be password-protected.

- Where possible, devices should also use encryption or secure cloud storage with two-factor authentication.

- Data files must not be stored on shared or public computers.

- When sending or sharing member data electronically, it should be by encrypted or password protected email attachments. **Passwords should be communicated separately**.

- Backups of important data (e.g. membership lists) must be stored securely and deleted once no longer required.

- Where office bearers use personal or consumer email or cloud services for legitimate RPOAS business, accounts must be secured using strong passwords and, where available, multi-factor authentication. Personal data held within such accounts must be limited to what is necessary for Association purposes and must be securely deleted or transferred when the office bearer leaves post.

- Office bearers must take reasonable care to prevent unauthorised disclosure of personal data, including making use of the Blind Carbon Copy (BCC) facility when sending group emails and ensuring personal data is not shared through unsecured or publicly accessible systems.

8.4. **Paper records**

- Paper records containing personal data (such as membership forms or attendance lists) must be stored in a locked cabinet or secure area when not in use.

- Paper records should not be left unattended in public or shared areas.

- Any paper records no longer required should be shredded or securely destroyed.

8.5. **Access control**

- Access to members personal data is limited to the post-holders as listed in section 5.2 above
- Each Branch must maintain awareness of who has access to members personal data and ensure permissions are withdrawn when individuals leave post.

8.6. **Incident reporting**

Any suspected loss, unauthorised access, or disclosure of personal data must be reported immediately to the national Secretary or to the national Assistant Secretary, who will assess the need for formal breach reporting. Contact email addresses for both are as follows:

National Secretary and Assistant Secretary contact details

- **rpoas-sec@rpoas.org.uk**
- **rpoas-assist-sec@rpoas.org.uk**

8.7. **Policy review**

RPOAS will review its data storage and security practices annually as part of the Certificate of Fitness process and will take reasonable steps to strengthen controls where risks are identified.

- - - - - - - - - - - - - - -

end