| SAMA 82 | Controlled Document |
|---|---|

# The South Atlantic Medal Association (1982)

## DATA PROTECTION POLICY

| | |
|---|---|
| **Policy Number** | 12 |
| **Document Owner** | SAMA (82) |
| **Ratifying Body** | Board Of Trustees |
| **Policy Lead** | Alan Dodsworth |
| **Available (upon approval) to** | Members |
| **Next Scheduled Review Date** | 14/10/2026 |

**POLICY CONTEXT & REQUIREMENT**

The Data Protection Policy has been developed to protect the organisation, its' employees, trustees and membership by ensuring the data it holds, is kept safe and used appropriately, in line with organisational objectives.

| Version Control | | | | |
|---|---|---|---|---|
| Version | Author | Status | Date | Change Detail |
| 1.0 | Andrew Lockett | Implemented | 14/10/2024 | N/A |
| 2.0 | Alan Dodsworth | Draft | 19/08/2026 | Addition of data protection complaints procedure (Section 33). Plus New Front Page, Policy Lead & Version Control |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

1. **Introduction**

1.1 The trustees have prepared this document to control the use and processing of data in compliance with General Data Protection Regulations. All Trustees, employees and volunteers should be aware of its requirements and adopt a culture of compliance with the care, control and management of personal data required by the regulations.

2. **Scope**

2.1 The scope of this document is focused around personal data.

2.2 Personal data means:

2.2.1 any information relating to an identified or identifiable person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number (eg social security number) or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (eg name and first name, date of birth, biometric data, finger prints, DNA).

2.3 Sound practices adopted for the management of personal data may be appropriate for other data. Where this is beneficial for efficiency, convenience or good communication it should be adopted.

3. **The Policy and objectives of the association are that:**

3.1 The association should reach full compliance with the standards and objectives of the data protection principles and the General Data Protection Regulations by:

3.1.1 fostering a culture of competent data management and data care particularly where the data involves personal data.

3.1.2 providing suitable training and generating competence in its trustees, employees and volunteers.

3.1.3 providing appropriate communication with those with whom it data shares setting out what they can, must and cannot do with the association's data.

3.1.4 putting in place measures to provide security against unlawful access, data escape, inappropriate processing, unnecessary holding of data and achieve appropriate consent from data subjects.

3.1.5 responding to data enquiries accurately and promptly and without disclosing personal data to other than the data subject.

3.1.6 conducting risk assessments relating to personal data and reviewing these periodically.

4. **Data protection principles (GDPR)**

4.1 Personal data shall be:

4.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

4.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.4 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;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes

or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

4.6 processed 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.

**5. References:**

5.1 General Data Protection Regulations 2018.

5.2 Data Protection Act (Legislated 1998, amended 2018 to incorporate GDPR).

**6. Acceptable basis for processing (including retaining and sharing)**

6.1 Legal obligation

6.2 Legitimate interest

6.3 Consent (the weakest and most troublesome)

6.4 Contract

6.5 Vital Interests

6.6 Public Tasks

**7. Communicating the policy**

7.1 Trustees are to take the lead in communicating the policy, and the measures required for implementation, to all within the association who deal with personal data. They will achieve this by:

7.1.1 running training sessions where a need is identified.

7.1.2 communicating instructions and methods.

7.1.3 seeking feedback from trustees, employees and volunteers.

7.1.4 carrying out internal audits.

7.1.5 making Data protection a recurring agenda item at meetings.

**8. Data Subjects**

8.1 A list of data subjects is given in Annex A.

8.2 A data subject is a person about whom the association holds personal data.

8.3 The annex describes the situations where personal data may be released or should be expected to be released to data sharers or the public domain. In all cases, where consent is needed, the permission for the data to be released must be provided by the data subject.

**9. Data Holders**

9.1 A list of data holders is given in Annex B

9.2 Data holders are key personnel within the organisation who manage and control personal data with or without the assistance of other persons.

**10. Risk Analysis**

10.1 A risk analysis is included with the list of data holders in Annex B.

10.2 The association shall prepare and document its analysis of risk in terms of likelihood and severity associated with non-compliance, revising and updating the analysis at suitable intervals. The association shall minimise the risk of non-compliance by good data management, processes, suitable security and paying heed to the risk analysis.

10.3 The risk assessment shall be assessed at regular intervals.

**11. Medal Holders List**

11.1 These are lists of medal holders from the MoD and are made up of service number, surname, forename or initial, date of birth, service, rank, ship, regiment or flight, date and place of killed in action.

11.2 This list is under the control of the Association Secretary.

11.3 Depending on the source, these lists may have very few of these data sets.

11.4 This list is necessary for continual retention as it defines the grant beneficiaries of the charity. The medal review of 2014 introduced a further category of medal holders who continue to be added to the medal list and become beneficiaries for grants.

**12. Membership List**

12.1 This is a list of persons who have paid a one-off entry fee to join the association.

12.2 The list may also contain members who were not required to pay a fee.

12.3 This list is under the control of the Association Secretary.

12.4 This data has been collected since 1997 on a form devised at the time.

12.5 In accordance with the Articles and Memorandum of the Association members become liable to pay off any debts of the association, should it fold, at the rate of £1 per member. It is therefore a requirement in company law to retain a list of members and their address and/or means of contact for this purpose. (Clause 5 - Articles).

12.6 Trustees should encourage members to update their membership details where there is a need. Of greatest value to the association is the replacement of the original means of communicating with the member such as electronic or postal address and telephone contact.

12.7 The list contains details of contact and address at the time of completion and application. Whilst this data is not out of date for the time of completion the contact details may no longer be appropriate if these have been changed without notifying the association.

**13. Beneficiary list**

13.1 Grants

13.1.1 Grants are provided in accordance with the charity objectives to beneficiaries (those who were part of the South Atlantic task groups 1982 and in the period thereafter until 21 October 1982). To obtain a grant, applicants must submit personal data supporting the need so that the Grant Sub Committee can assess the validity of the case and the extent of the grant payable.

13.1.2 The receipt and distribution of the information is managed at the association office.

13.1.3 The sub-committee analyses the facts but not the personal data and votes on the grant and the amount to be paid. See the Policy 20 Grant Procedure.

13.1.4 The applicant must agree to the use and sharing of the application data amongst the employees of SAMA82, the grant sub-committee, the treasurer and the chairman for the grant to be assessed. Grants applications without consent for limited distribution of the justification shall be parked until this issue is resolved.

13.1.5 The applicant must agree to the retention of that data for a maximum of 12 months after the grant has been paid in case of any recovery action should the application be found to have been corrupt or unfair.

13.1.6 The applicant must agree to the retention of a record of the payment in the accounts for a period of seven years to meet accounting standards.

13.2 Sponsorship

13.2.1 The association sponsors beneficiaries for discounted flights, on an availability basis, to the Falkland Islands. In this process the association acts as an agent for the Ministry of Defence.

13.2.2 Information is collected to enable the data sharers to carry out their part in the process of getting beneficiaries to and from the islands.

13.2.3 This process involves the MoD, RAF Brize Norton.

13.2.4 The applicant for sponsorship must give permission to share data collected for this purpose which may include other agencies essential for the orderly and safe travel and return including any diversions and delays that may be necessary.

13.2.5 The data is kept in the SAMA office.

13.2.6 Data subjects should be warned, in the data consent section, that this data is likely to reach places outside the European Economic Union for the purpose of the journey.

13.2.7 For the purpose of any unresolved insurance or liability issues the data shall be retained for 12 months at which time the data must be destroyed.

13.2.8 It is unlikely that a beneficiary can be sponsored without the collection and sharing of this data.

13.3 Events

13.3.1 Beneficiaries that participate in events such as the AGM, Dunkirk little ships, Remembrance Parade Whitehall and other similar recurring or non-recurring events will need to inform the association of data such as name, address, contact details, disabilities, dietary needs, travel mode, age, etc. The same will apply where a companion, wife, partner or similar is to engage in the same event. The same data rules would apply to both (or more) engaged in the event.

13.3.2 The attendees must permit the sharing of data with the association contractor to enable them to participate in the event.

13.3.3 The data must be destroyed within 28 days except where there is a liability issue in which case the data may be kept for up to one year.

13.3.4 This data is retained in the office.

13.3.5 It is unlikely that a beneficiary can be given access to all aspects of the event without the collection and sharing of this data.

**14. Employment**

14.1 Employees are required by law to provide personal information about domicile, right to work, tax and national insurance, previous employment, qualifications, references, and for some of this to be shared with pension providers and HMRC. The employer provides information on pay scales and rates, deductions and will keep records of ongoing interviews, training, sickness absence, performance and discipline.

14.2 This data processing will be justified under our legal obligations.

14.3 This information is held by the treasurer for financial matters and by the trustee supervising the office for matters of performance, training and discipline.

14.4 The treasurer retains the information for the duration of the employment as does the trustee supervising the office.

14.5 Payments made are retained in the accounts for seven years in compliance with the accounting standards.

14.6 Where an employee leaves, the information about the employment is destroyed after five years. The retention is for the purpose of answering calls for references. Where an employee is confident that a reference will never be required, the data will be destroyed after twelve months on request.

14.7 The treasurer's information is held on No 1 computer at his home address.

14.8 The trustee supervising the office on his or her computer at his home address.

14.9 The use of email to send Personal Identifiable Information (PID) should be done using caution or not at all. Email messages sent via the internet are not secure and could be intercepted, leaving the association liable under Data Protection Laws. For example sending an email from (for example) user1@sama82.org.uk to user2@sama.org.uk is safe because it does not leave the confines of our web server. An email from user1@sama82.org.uk to gmail.com or yahoo.com goes via the hostile network that is the internet.

**15. Correspondence**

15.1 Persons who correspond with the association must expect that their communication may be circulated to trustees, employees and regional staff unless their communication is marked confidential, in confidence or some other restrictive marking.

15.2 Where the correspondence is suspected of being confidential or it contains information of a personal nature then the sender is to be asked to give permission for the data to be shared with a list of specified persons.

15.3 Where that permission is not forthcoming then the correspondence is terminated and the communications are deleted.

15.4 Correspondence should be deleted 12 months after receipt unless there are any ongoing issues, in which case the correspondence should be retained and protected until the issue has been finally resolved followed by six months.

**16. Meeting Minutes**

16.1 Those who attend and contribute to minutes are included in the attendance list and may be referred to in the text of the minutes.

16.2 Persons attending meetings are required to give consent for their inclusion in the attendance list and in references to their contribution.

16.3 Minutes shall include a statement stating that attendees give permission for the circulation of the minutes and a record of their contribution to the meeting. The minutes will be deemed a matter of public access.

16.4 Where a meeting discusses confidential matters for which an attendee does not give permission for wider circulation then those minutes will be recorded as confidential and only made available to attendees who are to control the information as personal data.

**17. Data Sharers**

17.1 Data sharers are those bodies or persons with whom the organisation shares personal data.

17.2 Data sharers are to be given suitable directions on how they can use the data, who they can pass it on to, the protection required and the conditions under which the data is destroyed.

17.3 Data sharers are listed in annex C

17.4 Instructions to be given to data sharers;

17.4.1 you and your organisation are provided with this information to enable you to carry out the specific function required by the contract or agreement and for no other purpose;

17.4.2 the information is to be secured and managed so as to prevent access to it by any person who has no need to know;

17.4.3 on completion of the contract or agreement and a prudent time to enable corrections, the data is to be deleted by a means that prevents unauthorised access to the data;

17.4.4 where, through some legal obligation, you are required to make the information available to some third party you shall inform the association within a reasonable amount of time (normally the same day).

**18. Democratic and elective data subjects**

18.1 The trustees are responsible for the compliant democratic processes set down in the articles and memorandum of the association.

18.2 Appointments and Elections cannot proceed without personal information about candidates and appointees and for this information to be made available to members.

18.3 Candidates for all selective and elective posts are invited to supply information about themselves and for this information to be widely available to the point that it cannot be controlled.

18.4 All cvs or election manifestos shall be accompanied by a statement allowing this personal information unrestricted availability to the public. Where a candidate withholds this availability then it is unlikely that the candidate will be successful in an appointment or election but may proceed through the voting or selection process.

**19. Regional and area representatives**

19.1 Regional and area representatives shall inform the office of the personal data they hold, the means of storage and the use to which it is put.

19.2 The office is to assess the data and advise on the compliant means of storage, maintenance of accuracy and the timely destruction of the data.

**20. Volunteers**

20.1 Volunteers, other than transient volunteers, should have the following personal data recorded at the office and kept up to date whenever necessary.

20.1.1 Name.

20.1.2 Address.

20.1.3 Telephone.

20.1.4 Specialist skills.

20.1.5 Time or occasions when available.

20.1.6 Data on volunteers should be destroyed within one month of permanently ceasing to be a volunteer.

**21. Data Organisation**

21.1 Data Controller – Association Secretary.

21.2 Trustee data overseer – Trustee with responsibility for the Office.

**22. Gathering consent**

22.1 The association is to modify or generate suitable forms for the purpose of obtaining consent for all relevant aspects of its data holding.

22.2 These forms are to become an annex to the procedure.

22.3 Consent will be asked for in all new presentations of information by providing forms on the web site.

**23. Destruction of personal data**

23.1 Electronic.

23.1.1 Online submissions and emails shall be deleted in accordance with the destruction of paper records (Policy 15 Records- Retention and Destruction).

23.1.2 The timings stated for destruction of electronic records shall have a time zone allowance of -/+ 6 months.

23.2 Paper.

23.2.1 Paper records should be destroyed by in accordance with the destruction of paper records (Policy 15 Records- Retention and Destruction) the use of:

23.2.1.1 paper shredding by suitable machine,

23.2.1.2 burning,

23.2.1.3 removal by a suitable contractor.

23.2.2 The timings stated for destruction of paper records shall have a time zone allowance of -/+ 6 months.

**23. Data accuracy**

23.1. Whilst it is impossible, mainly through some time delay, for all data to remain accurate all of the time, data holders should endeavour to update personal data in reasonable time and in particular if the data is about to be used or has been requested.

23.2. Where a data enquiry is made a check of the data accuracy should be made and any corrections or updates applied.

**24. Internal audit and risk assessment**

24.1. Trustees can appoint a person to carry out a data management risk assessment or audit at intervals of between 1 and 4 years.

24.2. The internal inspection and review shall examine the processes, skills and arrangements and identify any strengths and weaknesses in the arrangements and management

**25. Corrective and remedial measures.**

25.1. The trustees have the responsibility to respond to observations of weakness, non-compliance or potential for improvements or strengthening the data management arrangements.

25.2. It is for trustees, led by the Chairman, to put in place the appropriate measures.

**26. Data Appointments.**

26.1. These appointments are made by the trustees to meet the organisational requirements.

**27. Physical protection.**

27.1. Computer storage

27.1.2. Office computers shall be located and secured within the office under the office security.

27.1.3. Computers shall be password protected and personal data files shall be further password protected with these passwords known only to the two employees. The passwords are to be written down, sealed within an envelope, suitably marked and placed within the key safe.

27.1.4. Passwords shall be changed at least monthly.

27.1.5. Office computers are protected by the same measures as for paper storage but are not locked in safes when not in use.

27.2. Paper storage

27.2.2. The office shall be secured with a suitable lock accepted by the landlord and with no more than three keys. The keys shall be held by each of the employees (one each). A third key should be held by the Trustee in charge of the office or retained in a key safe.

27.2.3. Documents containing personal data shall be stored in a suitably locked filing cabinet with the keys being placed in the key safe when not in use.

27.2.4. The key safe shall be checked to ensure it is locked on closing up the office and on opening the office. If the safe is not locked on opening the office the matter is to be reported to the chairman.

27.2.5. The main office is protected by suitable security measures.

28. **Responding to data enquiries.**

28.1. Responses for copies of personal data require careful preparation.

28.2. It shall be the duty of the Association Secretary to establish beyond reasonable doubt that the person requesting the data is the data subject. This shall be done by appropriate questioning ensuring that evidence presented conforms with the data held about the person.

28.3. The process may require calling back or writing by post to the applicant for further assurance.

28.4. If there is any doubt about the identity of the applicant the chairman should be informed.

28.5. The association has one calendar month in which to comply with the request for the data held. If however it is a complex case then further time can be allowed.

28.6. If the request is manifestly unfounded or excessive the association may refuse the request of charge for the administrative cost of preparing the response.

**29. Data subjects rights:**

29.1. to be informed.

29.2. of access.
29.3. to rectification.
29.4. to erasure.
29.5. to restrict processing.
29.6. to data portability.
29.7. to object.
29.8. not to be subject to automatic decision making including profiling.

**30. Privacy Notice**

30.1. A privacy notice shall be prepared based on the annexes generated.
30.2. The privacy notice was published in the first edition of the newsletter for 2018. No feedback was received but additional information will be required in due course.

**31. Information for SAMA 82 Annual report**

31.1. To meet the corporate norms the association shall include in its annual report, a report on the conduct of its data protection measures and any significant breaches. It should further indicate any plans for corrective and improvement measures.

**32. Advisory Information.**

32.1. As lessons are learned they should be added to Annex D, advisory information which gives guidance on methods and practices to follow.
32.2. These advisory notes should be numbered 1 onwards and reviewed at least annually and consolidated into notes for good practice.

**33. Data Protection Complaints Procedure.**

33.1. Data Protection complaints should be raised with the Trustee responsible for Data protection using the email address alan.dodsworth@sama82.org.uk.
33.2. SAMA 82 will acknowledge receipt of complaints, usually within 30 days of receipt.
33.3. SAMA 82 will report on our Data Protection Incident Report Log.
33.4. SAMA 82 will report on our Data Breach Log (if appropriate).
33.5. SAMA 82 will report the incident to the Information Commissions Office (ICO) if appropriate.
33.6. The Trustee responsible for Data Protection will investigate the complaint, while keeping all parties informed at all times. Once the investigation is complete, he/she will:
33.6.1 Implement any remedial actions that have arisen as part of the investigation.
33.6.2 Report findings to original complainant and trustees

| Annex A Data Protection - Annex A Data Subjects | | |
|---|---|---|
| Data Subjects | Nature | Data Kept and justifcation. |
| President | Appointed by the trustees - see procedures | The president would normally provide a curriculum vitea (cv) explaining his role in the conflict and a career history which he would give consent for it to be shared with beneficiaries and the public. The president would also provide address and contact information for whom he may give limited consent for distribution to necessary persons. This latter information would be subject to protection. |
| Officers of the Association | There are three officers of the association. The Chairman, Association Secretary and Treasurer. | There is a requirement in Company law for information and contact details to be available for the officers of the association on a public-wide basis. The release of all other information would be subject to data subject consent. |
| Trustees | These are elected by members at the AGM or co-opted by trustees where trustee places are gapped.. For the purpose of election the members require some information about the candidates for election. Candidates should make this information freely available and not subject to any data protection arrangements. | A candidate for election who withholds significant amounts of information relevant to the post of trustee is unlikely to get elected. A candidate must pass the fit and proper person test to become a trustee by completing a declaration required by the charity commission. A successful candidate who does not complete the declaration or fails to meet the requirement would be dismissed by the trustee board. The declaration is confidential data and must be properly protected. |
| Members | Persons who have joined under the rules of the association as they were at the time of joining or as revised on 1 May 2015 for those who joined after that date | Membership data as defined in the joining form and other data acquired during the process of communication. Members who participate in area and regional management may also provide additional information for which they must give appropriate consent for the information to be released. It is unlikely that a member could carry out these tasks without some release of contact information. There is a requirement in clause 5 of the Articles for the association to keep membership information. |
| Employees | Persons employed and former employees | Data necessary for the compliant employment, management and care of employees. This information is restricted to the officers of the association only, plus the trustee managing the office. This is sensitive information and includes bank details. It is necessary to keep this information throughout and, for a time, after completion of employment |
| Beneficiaries | Persons who are in receipt of the South Atlantic medal for service between 2 April 1982 and the 21 October 1982 | There are incomplete lists of medal holder's names held by the association without address and contact details. The association intends to keep this information since it carries with it no other personal data and has been in the public domain. Should any person wish to be removed from the association's list then such a request is welcomed. Without this information retained it is unlikely that the association will be able to respond quickly to a grant or membership request. The medal list provides independent verification of grant beneficiary qualification. |
| Beneficiaries in receipt of grants and/or sponsorship | Where grants and/or sponsorship is required the applicant will be asked more detailed information to justify receipt. This information will be the minimum required and shall be destroyed within 18 months of the provision of the grant or sponsorship | It is unlikely that the association will be able to provide the grant or sponsorship without the necessary information. Applicants must agree for the required amount of data sharing to enable the successful passage of the grant or sponsorship process. Such data will be destroyed 12 months of the successful completion of the grant or sponsored action unless some recovery or liability issue is outstanding. Since this information may contain medical, disability, employment and possibly criminal convictions this information is regarded as sensitive. |
| Volunteers | Volunteers are persons who may or may not be members but support the association in a productive role | Data on volunteers must be protected on the same basis as employees. Volunteers have names, contact details and addresses recorded and no other information is necessary. (Fact Check). Where a volunteer is a member then the treatment should be as a member. |
| Vice presidents | Vice presidents are appointed by trustees in accordance with procedure "HonVicePres" | Vice Presidents should provide a cv or review of the relevance of their experience to being a vice president of the association. This should be provided with personal release for the membership and the public. Nothing in the contents should be subject to ongoing data protection. |
| Correspondents | Persons who communicate with the association | The name and source address or contact contained in the correspondence should be regarded as freely available to trustees and employees. The permission of the sender should be requested to expand the distribution network of the correspondence. However, if a correspondence is marked in confidence, confidential, or some other restrictive statement then the correspondent shall be asked to whom, from a supplied list, they would allow access to the contents. Correspondents who do not allow sufficiently wide circulation may find that the subject matter is not dealt with. |

**Annex B Data Protection Data Holders and Risk Assessment**

| Data Holder | Nature of data | Where kept | Risk severity | Risk Likelihood | Actions required to minimise risk | Actions required |
|---|---|---|---|---|---|---|
| Treasurer | Records of wages, tax, national insurance, and student loans paid to HMRC | In HMRC Basic Paye work sheet for calculation of these payments. Work done on Treasurer's number 1 computer. Summary excel spread sheet. | Medium | Low | Appropriate encryption and password protection | Legal Obligation |
| Treasurer | Records of donations from members, other organisations and individuals | On treasurer's number 1 computer, at HSBC Bank and on paper copies of bank statements. | very low | Low | Household security and encryption | Legal Obligation |
| Association Secretary | List of membership details and personal information about service started in 1997 and continued thereafter. MoD Medal lists. Correspondence | Office on x Computer. Paper data | low | low | Office security, data encryptions, and password protection | Legitimate Interest |
| Association Secretary | List of recipients of newsletters other than members. | Office on x Computer. Paper data. Shared with printer | Low | Medium | This data is shared with the newsletter printer and must be provided with limiting conditions and instructions for destruction | Legitimate interest |
| Association Secretary | Applications for flights | Office and shared with MoD, Brize Norton, | | | Contain within the office | Consent / Also public tasks |
| Grant Committee chair | Details of the incomes and financial state of beneficiaries and other relevant issues such as health and family status applying for grants for the relief of themselves and dependents. | On computers in the office and computers of the grants committee, chairman and treasurer | Medium | low | Disconnect the name and means of identifying the claimant from the information justifying the grant so that information received from claimant is no longer personal data in circulation | Consent |
| Grant committee members | Details of the incomes and financial state of beneficiaries and other relevant issues such as health and family status applying for grants for the relief of themselves and dependents. | On computers of the committee member | Medium | low | Annonomise the data so that it is no longer personal data. | Consent |
| Association Secretary | President, vice presidents and Trustee personal details, time served, contact and address details | In office and with other trustees, members and beneficiaries | Low | Very Low | | Legitimate interest, legal obligation |
| Area Officers and Branches | Area data | Main Office, with local directories for contacting people | Low | Very Low | Send out conditions for dealing with SAMA data | Consent |
| Association Secretary | Attendees at Remembrance Sunday and other parades | Main Office, branch and regional computers: shared with the Royal British Legion, UJC | Low | Very Low | None more than office protection schemes | Consent |
| Association Secretary | Attendees at AGM and other events | Office on x Computer. Paper data. Shared with organiser. | Low | Low | Instructions to data sharer | Consent |
| Association Secretary | Confidential Minutes | Office on x Computer. Paper data | Medium | Low | None more than office protection schemes | Legitimate interest |
| Inspector of Accounts | Accounting information including payroll, donations, | On inspectors computer with some paper records | Very Low | Very Low | Same protection arrangements as treasurer. | Legal Obligation |
| Office Staff | All data that is used in the office | On office computer and paper files | Low | Low | Within office protection arrangement | Legitimate interest, legal obligation |

**ANNEX C - Data Protection - Data Sharing Arrangements**

| Data Sharing Organisation | Activity | Destruction by sharer | Legal obligation | Consent | Legitimate interest |
|---|---|---|---|---|---|
| MOD at Abbeywood – Flights | Flights | One Year after completion of flights | | yes | |
| SAFFA | Grants | One Year after completion of grant | | yes | |
| Brize Norton | Flights | One Year after completion of flights | | yes | |
| ADM Contractor – AGM booking forms | AGM and events | Two years after the AGM | | yes | |
| Printing Contractor – Printers Newsletters – Mailing Lists | Newsletter | Two weeks after completion of issue of newsletter | | | yes |
| HSBC Bank | Accounts | Seven years+ | Yes | | |
| Paypal | Accounts | Seven years+ | Yes | | |
| Office Computer Maintainers | Office Maintenance | Not taken away | | | yes |
| UJC | Remembrance Sunday | Two weeks after remembrance day | | yes | |
| Area Conference Venues | Area Management | Two weeks after annual conference | | yes | |
| HMRC | Employees | Not controlled by SAMA | Yes | | |
| HMRC | Gift Aid options | Not controlled by SAMA | Yes | | |
| Nest Pensions | Employees | Not Controlled by SAMA | Yes | | |
| Royal British Legion – Parade Application & Poppy Wreath Orders | Remembrance Sunday | Two weeks after remembrance day | | yes | |
| Association of Dunkirk of Little Ships – events | Events | Two weeks after event | | yes | |
| Not Forgotten Association - events | Events | Two weeks after event | | yes | |
| Non-routine events | Events | Two weeks after event | | yes | |
| Charity Commission | Governance | Not controlled by SAMA | Yes | | |
| Company House | Governance | Not controlled by SAMA | Yes | | |
| Inspector of accounts | Annual Inspection | Fifteen months after completion of annual inspection | Yes | | |

***Annex D Principles from the 1998 Act***

*1.1 Data protection principles from the 1998 Act.*

*1.1.1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:- at least one of the conditions in Schedule 2 is met, and,in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

*1.1.2 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.*

*1.1.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*

*1.1.4 Personal data shall be accurate and, where necessary, kept up to date.*

*1.1.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*

*1.1.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.*

*1.1.7 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.*

*1.1.8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

***2. Annex E Lawful basis for Processing***

*2.1 Consent*

*2.1.1 The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.*

*2.1.2 Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance your reputation.*

*2.1.3 Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard.*

*2.1.4 Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.*

*2.1.5 Explicit consent requires a very clear and specific statement of consent.*

*2.1.6 Keep your consent requests separate from other terms and conditions.*

*2.1.7 Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.*

*2.1.8 Be clear and concise.*

*2.1.9 Name any third party controllers who will rely on the consent.*

*2.1.10 Make it easy for people to withdraw consent and tell them how.*

*2.1.11 Keep evidence of consent – who, when, how, and what you told people.*

*2.1.12 Keep consent under review, and refresh it if anything changes.*

*2.1.13 Avoid making consent to processing a precondition of a service.*

*2.1.14 Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.*

*2.2 Contract*

*2.2.1 You can rely on this lawful basis if you need to process someone's personal data:*

*2.2.1.1 to fulfil your contractual obligations to them; or*

*2.2.1.2 because they have asked you to do something before entering into a contract (eg provide a quote).*

*2.2.2 The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.*

*2.2.3 You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning*

*2.3 Legal Obligation*

*2.3.1 You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.*

*2.3.2 This does not apply to contractual obligations.*

*2.3.3 The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.*

*2.3.4 You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.*

*2.3.5 You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.*

*2.4 Public Task*

*2.4.1 You can rely on this lawful basis if you need to process personal data:*

*2.4.1.1 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or*

*2.4.1.2 to perform a specific task in the public interest that is set out in law.*

2.4.2 *It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.*

2.4.3 *You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.*

2.4.4 *The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.*

2.4.5 *Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.*

2.5 *Legitimate Interests*

2.5.1 *Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.*

2.5.2 *It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.*

2.5.3 *If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.*

2.5.4 *Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.*

2.5.5 *There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:*

2.5.5.1 *identify a legitimate interest;*

2.5.5.2 *show that the processing is necessary to achieve it; and*

2.5.5.3 *balance it against the individual's interests, rights and freedoms.*

2.5.6 *The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.*

2.5.7 *The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.*

2.5.8 *You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.*

2.5.9 *Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.*

2.5.10 *You must include details of your legitimate interests in your privacy notice.*

***3. Annex F Privacy Notice***

*3.1 The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.*

*3.2 What information must be supplied?*

*3.2.1 The GDPR sets out the information that you should supply and when individuals should be informed.*

*3.2.2 The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.*

*3.3 The information you supply about the processing of personal data must be:*

*3.3.1 concise, transparent, intelligible and easily accessible;*

*3.3.2 written in clear and plain language, particularly if addressed to a child; and*

*4. free of charge.*

The table below summarises the information you should supply to individuals and at what stage.

| **What information must be supplied?** | **Data obtained directly from data subject** | **Data not obtained directly from data subject** |
|---|---|---|
| Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer | ✓ | ✓ |
| Purpose of the processing and the lawful basis for the processing | ✓ | ✓ |
| The legitimate interests of the controller or third party, where applicable | ✓ | ✓ |
| Categories of personal data | | ✓ |
| Any recipient or categories of recipients of the personal data | ✓ | ✓ |
| Details of transfers to third country and safeguards | ✓ | ✓ |
| Retention period or criteria used to determine the retention period | ✓ | ✓ |
| The existence of each of data subject's rights | ✓ | ✓ |
| The right to withdraw consent at any time, where relevant | ✓ | ✓ |
| The right to lodge a complaint with a supervisory authority | ✓ | ✓ |
| The source the personal data originates from and whether it came from publicly accessible sources | | ✓ |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data | ✓ | |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences | ✓ | ✓ |

| | | |
|---|---|---|
| When should information be provided? | At the time the data are obtained. | Within a reasonable period of having obtained the data (within one month) |
| | | If the data are used to communicate with the individual, at the latest, when the first communication takes place; or |
| | | If disclosure to another recipient is envisaged, at the latest, before the data are disclosed. |

| | | | | | |
|---|---|---|---|---|---|
| Approved by | SAMA 82 Trustees | Policy owner | SAMA 82 | Available to | Members |
| Original Approval date | 14.10.24 | Original Written by | Andrew Lockett | Review Date | 14.10.26 |
| Amendment Issue Number | Issue 2/2 | Amended by | Alan Dodsworth | Amendment date | 26.05.26 |