

General Personal Data Protection Policy

Document Ref. GPDPP

Version: 1.0

Draft 1

Document Author: **William Despard** (Data Protection Officer-DPO)

Contents

1. Scope, Purpose and Users	3
2. Reference Documents	3
3. Definitions	4
4. Basic Principles Regarding Personal Data Processing	5
4.1 Lawfulness, Fairness and Transparency	6
4.2 Purpose Limitation.....	6
4.3 Data Minimisation.....	6
4.4 Accuracy	6
4.5 Storage Period Limitation	6
4.6 Integrity and confidentiality	6
4.7 Accountability	7
5. Building Data Protection in Business Activities.....	7
5.1 Notification to Data Subjects.....	7
5.2 Data Subject's Choice and Consent	8
5.3 Collection	8
5.4 Use, Retention, and Disposal	8
5.5 Disclosure to Third Parties	8
5.6 Cross-border Transfer of Personal Data.....	9
5.7 Rights of Access by Data Subjects.....	9
5.8 Data Portability	10
5.9 Right to be Forgotten.....	10
6. Fair Processing Guidelines	10
6.1 Notices to Data Subjects	10
6.2 Obtaining Consents.....	10
7. Organisation and Responsibilities	11
8. Response to Personal Data Breach Incidents.....	12
9. Audit and Accountability.....	13
10. Conflicts of Law	13
11. Managing records kept on the basis of this document.....	14
13. Validity and Document Management	15
14. Revision History	16

1. Scope, Purpose and Users

The Army and Navy Club, hereinafter referred to as the “Club”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Club operates. This Policy sets forth the basic principles by which the Club processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Club and its third parties processing the personal data of data subjects within EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Club.

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Act 2018 (DPA 2018)
- Employee Personal Data Protection Policy
- Data Retention Policy
- Data Protection Officer Job Description
- Personal Data Inventory Guidelines
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Guidelines
- Cross Border Personal Data Transfer Procedure
- Information Security Policy
- Breach Notification Procedure

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject") 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.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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 any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single

establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR;

Lead supervisory authority: The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of the EU GDPR;

Each “**local supervisory authority**” will still maintain in its own territory and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers include conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

“**Main establishment as regards a controller**” with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

“**Main establishment as regards a processor**” with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Group Undertaking: Any holding Company together with its subsidiary.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

4.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of the following 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Club can **fulfil a contract** with the individual, or the individual has asked the Club to take specific steps before entering into a contract
- The data needs to be processed so that the Club can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed for the **legitimate interests** of the Club or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear **consent**

4.2 Purpose Limitation

We will only collect personal data for specified, explicit and legitimate reasons. We explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff will only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they will ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule/records management policy.

4.3 Data Minimisation

All Personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Club may apply anonymization or pseudonymisation to personal data if possible to reduce the risks to the data subjects concerned.

4.4 Accuracy

All Personal data processed is accurate and, where necessary, kept up to date; reasonable steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

4.5 Storage Period Limitation

Personal data will be kept for no longer than is necessary for the purposes for which the personal data is processed. This can be referenced in our Data Retention Policy.

4.6 Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Club applies appropriate technical and organisational measures to process Personal Data in a manner that ensures

appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the Club's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our Club and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

4.7 Accountability

The Club as a Data controller is responsible for and is able to demonstrate compliance with the principles outlined above.

5. Building Data Protection in Business Activities

In order to demonstrate compliance with the principles of data protection, the Club has built data protection into its business activities.

5.1 Notification to Data Subjects

(See the Fair Processing Guidelines section.)

5.2 Data Subject's Choice and Consent

(See the Fair Processing Guidelines section.)

5.3 Collection

The Club strives to collect the least amount of personal data possible. If personal data is collected from a third party, DPO will ensure that the personal data is collected lawfully.

5.4 Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data are consistent with the information contained in the General Data Protection Notice. The Club will maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data are used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. DPO is responsible for compliance with the requirements listed in this section.

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access club computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Staff, who store personal information on their personal devices are expected to follow the same security procedures as for club-owned equipment (see our ICT policies on acceptable use, Use of Social Media, and e-Safety)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 5.5)

5.5 Disclosure to Third Parties

Whenever the Club uses a third-party supplier or business partner to process personal data on its behalf, DPO will ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor GDPR Compliance Questionnaire will be used. We will establish a data sharing agreement with the supplier or contractor, to ensure the fair and lawful processing of any personal data we share.

The Club will contractually require the supplier or business partner to provide the same level of data protection as the club provides. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Club or upon the instructions of the Club and not for any other purposes. When the Club processes personal data jointly with an independent third party, the Club will explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

5.6 Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards will be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorisation from the relevant Data Protection Authority will be obtained. The entity receiving the personal data must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

5.7 Rights of Access by Data Subjects

Acting as a data controller, DPO is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and it allows them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

Confirmation that their personal data is being processed

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

A data subject access request form will be sent to the individual.

If staff receive a subject access request they must immediately forward it to the DPO.

5.8 Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit that data to another controller, for free. DPO is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

5.9 Right to be Forgotten

Upon request, Data Subjects have the right to obtain from the Club the erasure of its personal data. When the Club is acting as a Controller, DPO will take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

6. Fair Processing Guidelines

Personal data must only be processed when explicitly authorised by DPO.

The Club will decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

6.1 Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, DPO is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Club's security measures to protect personal data. This information is provided through General Data Protection Notice.

Where personal data is being shared with a third party, DPO must ensure that data subjects have been notified of this through a General Data Protection Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the General Data Protection Notice will reflect this and clearly states to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, the Data Protection Officer will make sure that the General Data Protection Notice explicitly states the purpose for which this sensitive personal data is being collected.

6.2 Obtaining Consents

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, DPO is responsible for retaining a record of such consent. DPO is responsible for providing data

subjects with options to provide the consent and must inform and ensure that their consent can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, DPO will ensure that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy personal data records, DPO will ensure that these requests are handled within a reasonable time frame. DPO will also record the requests and keep a log of these.

Personal data will only be processed for the purpose for which they were originally collected. In the event that the Club wants to process collected personal data for another purpose, the Club will seek the consent of its data subjects in clear and concise writing. Any such request will include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request will also include the reason for the change in purpose(s). The Data Protection Officer is responsible for complying with the rules in this paragraph.

Now and in the future, DPO will ensure that collection methods are compliant with relevant law, good practices and industry standards.

DPO is responsible for creating and maintaining a Register of the General Data Protection Notices.

7. Organisation and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with the Club and has access to personal data processed by the Club.

The key areas of responsibilities for processing personal data lie with the following organisational roles:

The board of directors or other relevant decision-making body makes decisions about, and approves the Club's general strategies on personal data protection.

The **Data Protection Officer (DPO) or any other relevant employee**, is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies, as defined in Data Protection Officer Job Description;

The **Data Protection Officer**, monitors and analyses personal data laws and changes to regulations, develops compliance requirements, and assists business departments in achieving their Personal data goals.

The **IT Manager**, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The **Marketing Manager**, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with the Data Protection Officer to ensure marketing initiatives abide by data protection principles.

The **Human Resources Manager** is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing Personal data protection expertise and awareness training for employees working with personal data.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

The **Departmental Managers/Heads** are responsible for passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The **Departmental Managers/Heads** must ensure that the Club reserves a right to audit suppliers.

8. Response to Personal Data Breach Incidents

When the Club learns of a suspected or actual personal data breach, DPO must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach Policy. Where there is any risk to the rights and freedoms of data subjects, the Club must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

When the personal data breach or suspected data breach affects personal data that is being processed by the Company as a data controller, the following actions are performed by the Data Protection Officer:

- The Club must establish whether the personal data breach should be reported to the Supervisory Authority.
- In order to establish the risk to the rights and freedoms of the data subject affected, the Data Protection Officer must perform the Data Protection Impact Assessment on the processing activity affected by the data breach.

- If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. However, the data breach should be recorded into the Data Breach Register.
- The Supervisory Authority must be notified with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.

DPO will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

9. Audit and Accountability

The Audit Department or other relevant department is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

10. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which the Army and Navy Club operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

11. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Subject Consent Forms	[specify folder on the Club Intranet or the database in your information system]	Data Protection Officer	Only authorized persons may access the forms	10 years
Data Subject Consent Withdrawal Form	[specify folder on the Club Intranet or the database in your information system]	Data Protection Officer	Only authorized persons may access the forms	10 years
Parental Consent Form	[specify folder on the Club Intranet or the database in your information system]	Data Protection Officer	Only authorized persons may access the forms	10 years
Parental Consent Withdrawal Form	[specify folder on the Club Intranet or the database in your information system]	Data Protection Officer	Only authorized persons may access the forms	10 years
Supplier Data Processing Agreements	[specify folder on the Club Intranet]	Data Protection Officer	Only authorized persons may access the folder	5 years after the agreement has expired
Register of General Data Protection Notices	[specify folder on the Club Intranet]	Data Protection Officer	Only authorized persons may access the folder	Permanently

13. Validity and Document Management

This document is valid as of 22nd May 2018.

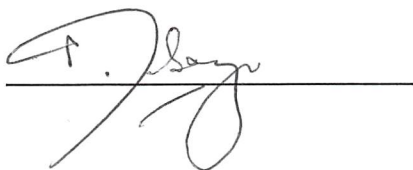
The owner of this document is DPO, who must check and, if necessary, update the document at least once a year.

DPO (Data Protection Officer)

William Despard

36-39 Pall Mall

London SW1Y 5JN

A handwritten signature in black ink, appearing to read 'A. de Souza', is written over a horizontal line.

Ayres de Souza, Club Secretary

14. Revision History

Version	Date	RFC Number	Summary of Changes
1.0	May 2018	GDPP	

Document Review

Date of Next Scheduled Review
May 2019

Distribution

Name	Title

Approval

Name	Position	Signature	Date