NARPO

DATA PROTECTION POLICY

March 2017

CONTENTS

CLAUSE

1. Policy statement 3
2. About this policy 3
3. Definition of data protection terms 3
4. Data protection principles 4
5. Fair and lawful processing 5
6. Processing for limited purposes 5
7. Notifying data subjects 6
8. Adequate, relevant and non-excessive processing 6
9. Accurate data 6
10. Timely processing 6
11. Processing in line with data subject's rights 6
12. Data security 7
13. Branch specific issues 6
14. Transferring personal data to a country outside the EEA 7
15. Disclosure and sharing of personal information 9
16. Dealing with subject access requests 9
17. Changes to this policy 10

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. We collect, store and process personal data about our members, employees, volunteers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and help ensure that we discharge our legal obligations appropriately.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 This policy has been written at the direction of the National Executive Committee. Any breach will be taken seriously and may result in disciplinary action being taken.

2.2 The types of personal data that we may be required to handle include information about current, past and prospective employees, members and volunteers, their families, and others, with whom we communicate. This personal data, which may be held on paper or on a computer or other media, is subject to the legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.6 The Data Protection Compliance Manager is responsible for ensuring overall compliance with the Act and with this policy. That post is held by the Deputy CEO of NARPO, 01924 362166, email depceo@narpo.org . Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager. However, given the nature of our structure the Data Protection Compliance Manager shall need to be able to rely on the support and assistance of each branch secretary. Consequently, the branch secretary of each branch within the association shall also be responsible for ensuring compliance with this policy at their branch.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. NARPO HQ and the Branch Secretaries are the data controllers of all the personal data used in our organisation.

3.5 **Data users** are those of our employees, Branch Officials and Members whose work involves processing personal data for NARPO purposes. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it is likely to include any others that handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles set out in the Act. These provide that personal data must be:

1. Processed fairly and lawfully.
2. Processed for limited purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate.

5. Not kept longer than necessary for the purpose.
6. Processed in line with data subjects' rights.
7. Secure.
8. Not transferred to people or organisations situated in countries without adequate protection.

We shall comply with the 8 Data Protection Principles. This will be achieved by our employees as part of their contract of employment. We also expect the same of our members and volunteers in accordance with the Rules of the Association.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that such processing is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data, as data controllers, we must ensure that these requirements are met.

5.3 **Security protocols must be observed when communicating, transferring or storing personal data. This prohibits sending personal data by non-secure email i.e. up to date virus protection and firewalls need to be in place, or to store that data on removable storage devices, such as USB sticks or discs.**

6. PROCESSING FOR LIMITED PURPOSES

6.1 We collect and process personal data, including data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources.

6.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

6.3 If you become aware of us processing personal data for any reason other than those listed in the Schedule please notify the Data Protection Compliance Manager, because he will either need to update the details of our registration as a data controller with the Information Commissioner's Office and/or take steps to ensure that data processing beyond the scope of the reasons set out in the Schedule ceases.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 We will inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data. At a Branch level, the Branch Secretary will be responsible for ensuring compliance and conduct an annual dip sampling audit of its members' records.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

It is important to ensure that personal data is stored appropriately using approved and audited systems, and periodically destroyed. The Act requires personal data be kept no longer than is necessary for the purposes for which it was collected

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also paragraph 16).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also paragraph 9).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

12.1 We will take appropriate security measures, taking cognisance of the following-

Potential harm- NARPO will ensure appropriate levels of security, having regard to the harm that may result from unauthorised or unlawful processing, accidental loss, damage or destruction and the nature of the data to be protected. At the same time, regard will be given to the state of technological development and implementation cost.

Employees, Branch Officials and Members acting for NARPO purposes- NARPO has a responsibility to take reasonable steps to ensure that the employees Branch Officials and Members acting for NARPO purposes, who have access to personal data, are reliable. This will also extend to reliability of data processor employees, ranch Officials and Members acting for NARPO purposes

Data processor security- when choosing data processors, NARPO will ensure it provides sufficient guarantees, in respect of the technical and organisational security measures. This will govern the data processors processing for the data controller and ensure that the data processor complies with those measures.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. **Personal data should therefore be stored on our central computer system "Supersleuth" and not on individual PCs or other storage devices e.g. mobile phones and tablets.**

12.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

(e) **Passwords.** Passwords should be changed regularly and kept confidential.

13. BRANCH SPECIFIC ISSUES

13.1 All Personal data should only be entered, stored, managed, handled or processed using the central Supersleuth database.

13.2 **Storage, processing, managing, handling and processing of personal data other than on Supersleuth is discouraged and should be a rare exception and not the rule.** Written permission must be obtained from Branch Secretary prior to any action operating outside of this policy. If approved, the Branch Secretary will notify the Data Protection Compliance Manager.

13.3 To the extent that, as at March 2017, personal data has been processed at Branch level, without the express permission of the Data Protection Compliance Manager/Branch secretary having been obtained, then the employee, member or volunteer that has dealt with personal data in this way must securely destroy those versions of the personal data (e.g. any database being a subset of the Supersleuth database), if they are no longer required or notify the Data Protection Compliance Manager/Branch secretary immediately.

13.4 Please keep in mind that the Act applies equally to personal data held at branch level, outside Supersleuth, just as much as it does to the personal data in Supersleuth. Consequently, those persons dealing with personal data outside Supersleuth must, in addition to obtaining express permission in accordance with paragraph 13.2, ensure that the Act and this policy are fully observed and complied with in respect of such personal data.

13.5 Keeping personal data on removable storage devices such as USB sticks or discs is potentially high risk and should be avoided, wherever possible]. In any event, sensitive personal data should never be stored on removable storage devices.

13.6 Branch secretaries shall be responsible for ensuring that all new employees [and any other persons] who may have access to personal data receive appropriate training and a copy of our current Data Protection Policy as part of their induction.

14. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

14.1 We may transfer personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

15. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

15.1 We may disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

15.2 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

16. DEALING WITH SUBJECT ACCESS REQUESTS

16.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees, and Branch Secretaries who receive a written request should forward it to the Data Protection Compliance Manager immediately.

16.2 We will charge an administration fee in return for dealing with a subject access request, which is payable in advance. As at the date hereof that fee is £10 but may increase over time.

16.3 We will deal with the subject access request within 40 days of the later of receiving payment of the administration fee and the details we reasonably require from the data subject in order to comply with their subject access request.

16.4 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

16.5 Our employees and Branch Secretaries will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16.6 Should legal proceedings be issued against us in relation to the Act they must be referred to the Data Protection Compliance Manager immediately.

17. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.