Data Protection Policy

1. INTRODUCTION

As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities (Name of Organisation) ((NAME OF ORGANISATION)) will collect, store and process personal data, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The types of personal data that (NAME OF ORGANISATION) may be required to handle include information about current, past and prospective employees, volunteers, customers, clients, suppliers or agents of (NAME OF ORGANISATION). The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how (NAME OF ORGANISATION) may process personal data, and a breach of the Act could give rise to criminal sanctions as well as bad publicity.

The purpose of this policy is to enable (NAME OF ORGANISATION) to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect (NAME OF ORGANISATION)'s supporters, staff and other individuals, and
- protect the organisation from the consequences of a breach of its responsibilities.

(NAME OF ORGANISATION) will:

- comply with both the law and good practice;
- respect individuals' rights;
- be open and honest with individuals whose data is held, and
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

2. STATUS OF THE POLICY

This policy sets out (NAME OF ORGANISATION)'s rules on data protection and the eight data protection principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data.

(NAME OF ORGANISATION)'s Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy. The Data Protection Compliance Officer is James Johnson, (NAME OF ORGANISATION) Deputy Chief Officer. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Compliance Officer.

This policy is not part of the contract of employment and (NAME OF ORGANISATION) may amend it at any time. However, it is a condition of employment that employees and others who obtain,

handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.

Any employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with their line manager and (NAME OF ORGANISATION)'s Data Protection Compliance Officer in the first instance.

This policy applies to:

- the Chief Officer of (NAME OF ORGANISATION)
- its branches and regions
- all paid staff and volunteers
- all sessional workers operating on behalf of (NAME OF ORGANISATION)

Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

3. DEFINITION OF DATA PROTECTION TERMS

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects: for the purpose of this policy include all living individuals about whom (NAME OF ORGANISATION) holds 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.

Personal data: means data relating to a living individual who can be identified from that data (or from that data and other information in possession of (NAME OF ORGANISATION)). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would still fall within the scope of the Data Protection Act 1998.

Data controllers: are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. (NAME OF ORGANISATION) is the data controller of all personal data used in its business.

Data users: include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following (NAME OF ORGANISATION)'s data protection and security policies at all times.

Data processors: include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on (NAME OF ORGANISATION)'s behalf.

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.

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 of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

4.1 FAIR AND LAWFUL PROCESSING

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case (NAME OF ORGANISATION)), who the data controller's representative is (in this case the Data Protection Compliance Officer), the purpose for which the data is to be processed by (NAME OF ORGANISATION), and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing (but consent can be implied in certain limited circumstances), or that the processing is necessary 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. In most cases the data subject's explicit consent to the processing of such data will be required.

4.2 PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose

for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

4.3 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

4.4 ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

(NAME OF ORGANISATION) will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

4.5 TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from (NAME OF ORGANISATION)'s systems when it is no longer required.

4.6 PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights.

(NAME OF ORGANISATION) is committed to ensuring that, in principle, Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff: in the staff handbook
- Volunteers: in the volunteer support pack
- Sessional workers: in the staff handbook
- Members: in the welcome pack
- Supporters: when they sign up (on paper, on line or by phone) for services or purchase products.

Information about members and supporters will only be made public with their consent. (This includes photographs.)

(NAME OF ORGANISATION) may receive information from an external organisation which contains personal information about the members of that organisation who are not members or supporters of (NAME OF ORGANISATION). For example, grant applicant/recipient organisations may supply (NAME OF ORGANISATION) with personal information on beneficiaries of organisations perhaps in case studies or reports. (NAME OF ORGANISATION) will only process such data where the organisation supplying this information confirms in writing that the data subject has consented to the use and storage of that information by (NAME OF ORGANISATION).

'Sensitive' data about members and supporters (including health information) will be held only with the knowledge and consent of the individual.

Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

5. DATA SECURITY

(NAME OF ORGANISATION) must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires (NAME OF ORGANISATION) to 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 may only be transferred to a third-party data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

- **Entry controls:** Any stranger seen in entry-controlled areas should be reported.
- **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).
- **Methods of storage:** Archived paper records of members are stored securely off site.

- **Methods of disposal:** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- **Equipment:** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off (manually or automatically) from their PC when it is left unattended for any period.
- **Passwords and Encryption**: Passwords/encryption/software packages are used to safeguard databases and removable media.

6. CONFIDENTIALITY

Because confidentiality applies to a much wider range of information than Data Protection, (NAME OF ORGANISATION) has a separate Confidentiality Policy.

Staff, volunteers and sessional workers will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

Where anyone within (NAME OF ORGANISATION) feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented.

7. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information (NAME OF ORGANISATION) holds about them must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Officer immediately.

When receiving telephone enquiries, employees should be careful about disclosing any personal information held on (NAME OF ORGANISATION)'s systems. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked.
- Refer to their line manager or the Data Protection Compliance Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

8. DIRECT MARKETING

(NAME OF ORGANISATION) will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting any (NAME OF ORGANISATION) services;
- promoting branch events;
- promoting membership to supporters;
- promoting sponsored events and other fundraising exercises;
- marketing the products of (NAME OF ORGANISATION), and
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out.

(NAME OF ORGANISATION) has the policy of sharing lists (or carrying out joint or reciprocal mailings) only on an occasional and tightly-controlled basis. Details will only be used for any of these purposes where the Data Subject has been informed of this possibility, along with an option to opt out, and has not exercised this option.

(NAME OF ORGANISATION) undertakes to obtain external lists only where it can be guaranteed that the list is up to date and those on the list have been given an opportunity to opt out.

(NAME OF ORGANISATION) will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

9. STAFF TRAINING AND RESPONSIBILITIES

Information for staff and sessional workers is contained in the staff handbook.

All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.

Data Protection will be included in foundation training for volunteers and sessional workers.

(NAME OF ORGANISATION) will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Consent will normally not be sought for most processing of information about **staff** and **sessional workers**, with the following exceptions:

- Staff details will only be disclosed for purposes unrelated to their work for (NAME OF ORGANISATION) (e.g. financial references) with their consent.
- Sessional workers, or other staff working from home, will be given the choice over which contact details are to be made public.

Information about **volunteers** will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

10. POLICY REVIEW

This policy is a living document and will be monitored and updated on an ad hoc basis where required by the Data Protection Compliance Officer, but a formal review will be undertaken every two years.

Presented to Personnel Subcommittee: **Suggested Review:**

Signed: _____ Date _____

Chair of Personnel

Signed: _____ Date _____
Chair of (NAME OF ORGANISATION)

Privacy statement

When you request information from (NAME OF ORGANISATION), sign up to any of our services or buy things from us, (NAME OF ORGANISATION) obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the Data Protection Act to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

We would also like to contact you in future to tell you about other services we provide, and ways in which you might like to support (NAME OF ORGANISATION). You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

Occasionally we carry out a joint mailing with carefully selected other organisations, in order to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, either ask for an application form to be sent to you, or write to the Data Protection Officer at (NAME OF ORGANISATION), (address). There is a charge of £10 for a copy of your data (as permitted by law). We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

Confidentiality statement for staff and volunteers

When working for (NAME OF ORGANISATION), you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are supporters or otherwise involved in the activities organised by (NAME OF ORGANISATION).
- Information about the internal business of (NAME OF ORGANISATION).
- Personal information about colleagues working for (NAME OF ORGANISATION).

(NAME OF ORGANISATION) is committed to keeping this information confidential, in order to protect people and (NAME OF ORGANISATION) itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by (NAME OF ORGANISATION) to be made public. Passing information between a branch and the head office, or between (NAME OF ORGANISATION) and a mailing house, or *vice versa* does not count as making it public, but passing information to another organisation does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information between the head office and branches;
- not gossip about confidential information, either with colleagues or people outside (NAME OF ORGANISATION);
- not disclose information – especially over the telephone – unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for (NAME OF ORGANISATION).

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: **Date:**