Data Protection Policy

Introduction

Labrador Retriever Rescue Scotland SCIO (SC042724) is a Scottish Charitable Incorporated Organisation and Kennel Club Approved Rescue. The Rescue's mission is to rescue, rehabilitate and rehome Labrador Retrievers and promote and advance responsible pet ownership. The Rescue also prevents rehoming by providing training and support to owners.

The Rescue needs to gather and use certain information about individuals. These can include people who wish to adopt or give up a Labrador Retriever, referees, suppliers, business contacts, volunteers and other people the Rescue may need to contact or with whom it has a relationship. This policy describes how personal data is collected, handled and used by the Rescue.

Why this policy exists

This data protection policy ensures that the Rescue:

- complies with data protection law and follows good practice
- protects the rights of volunteers, customers and others
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations - including the Rescue - must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles, which say that personal data must:

1. be processed fairly and lawfully
2. be obtained only for specific, lawful purposes
3. be adequate, relevant and not excessive
4. be accurate and kept up to date
5. not be held for any longer than necessary
6. processed in accordance with the rights of data subjects
7. be protected in appropriate ways
8. not be transferred outside of the European Economic Area, unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to all staff and volunteers of the Rescue; and all contractors, suppliers and other people working on behalf of the Rescue. It applies to all data that the Rescue holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- information on pets previously owned or homed

Sensitive personal data includes racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation. The Rescue may request some information on an individual's health status in order to identify whether he/she would be a suitable person with whom to rehome a Labrador Retriever or to match an individual with a Labrador Retriever. It does not collect other sensitive personal data.

If an applicant to adopt a Labrador Retriever obtains an animal elsewhere, the individual's data is deleted from the Rescue's records. If it has not proved possible to match an individual with a suitable Labrador Retriever, information about that individual is deleted from the Rescue's records after six months, unless the individual requests otherwise and the Rescue agrees. When an individual is matched with a Labrador Retriever, information about that individual and about the original owner of the Labrador Retriever will be retained (on paper, not electronically) until the death of the Labrador Retriever.

The Rescue does not carry out automated decision-making (including profiling).

Responsibilities

Everyone who volunteers or works for or with the Rescue has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone handling personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Trustees are ultimately responsible for ensuring that the Rescue meets its legal obligations, but Mrs Carolyne Poulton has day-to-day responsibility for the following:

- Keeping the Trustees updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies
- Handling data protection queries
- Dealing with requests from individuals to see the data the Rescue holds about them ("subject access requests")
- Checking and approving any contracts or agreements with third parties that may handle the Rescue's sensitive data
- 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
- Evaluating any third-party services the Rescue is considering using to store or process data (eg cloud computing services)
- Approving any data protection statements attached to communications such as emails and letters

General guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- The Rescue will provide training to help volunteers understand their responsibilities when handling data.
- All data should be kept secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Rescue or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data usually stored electronically but printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Paper and printouts should not be left where unauthorised people could see them (eg on a printer).
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removeable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Rescue's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

- When someone is working with personal data, the screens of their computers should always be locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Copies of personal data should not be saved to personal computers. Always access and update the central copy of any data.

Data accuracy

The law requires the Rescue to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of everyone who works with data to take reasonable steps to ensure that it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Unnecessary additional data sets should not be created.
- Every opportunity should be taken to ensure data is updated (eg by confirming a customer's details when they call).
- Data should be updated as inaccuracies are discovered. For instance, if an individual can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the Rescue are entitled to:

- Ask what information the Rescue holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the SCIO is meeting its data protection obligations.

If an individual contacts the Rescue requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to Mrs Poulton at carolynepoultonlabs@gmail.com. Mrs Poulton will always verify the identify of anyone making a subject access request before handing over any information, and will aim to provide the relevant information as soon as possible but in any event within one month of receipt of the request.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Rescue will disclose requested data. However, Mrs Poulton will ensure the request is legitimate, seeking assistance from the Trustees and from the Rescue's legal advisers where necessary.