RNARS

DATA PROTECTION POLICY

Policy prepared by: **David Firth**

Approved by: **The Committee:** _____/_____/_____

Policy became operational on: _____/_____/_____

Next policy review date: _____/_____/_____

Draft Document for inclusion into the constitution

17th November 2017

CONTENTS

INTRODUCTION

Why we need a data protection policy

UK data protection law cannot be ignored under any circumstances. The Data Protection Act 1998 applies to every business that collects, stores and uses personal data relating to customers, staff or other individuals. Failing to comply could mean a fine of up to £500,000.

A clear data protection policy makes sure everyone understands why data protection is important. It also describes procedures for collecting, working with and storing data.

Why this policy exists

This data protection policy ensures that the RNARS:

- **Complies with data protection law and follows good practice**
- **Protects the rights of members, the Committee and affiliates**
- **Is open about how it stores and processes individuals' data**
- **Protects itself from the riskes of a data breach**

Data Protection Law

The Data Protection Act 1998 describes how all organisations including the RNARS must handle and store personal information.

These rules apply regardless of whether data is stored electronicall, 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 as shown below:

Data protection policy structure

The Data Protection Act is founded on eight principles of data protection. 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 the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Our data protection policy is organised along similar lines, addressing each of these principles to explain:

- To what types of data the policy applies.
- Who in the business is responsible for data protection.
- The main data risks faced by the Society.
- Key precautions to keep data protected.
- How data should be stored and backed up.
- How the company ensures data is kept accurate.
- What to do if an individual asks to see their data.
- Under what circumstances the business discloses data, and to whom.
- How the company keeps individuals informed about data it holds.

Implementing our data protection policy

Our data protection policy is a practical document that should enable members to understand it and refer to it when they need data protection advice. Our data protection policy is regularly reviewed and amended when changes occur to the way we operate or when we plan to start storing data in a new way. All members are required to read our data protection policy and sign a document to that end when introduced. This document forms a part of our joining process for new members. However, always remember that a policy alone is not enough to ensure your business keeps its data safe and operates within the law. Training, expert advice and clear lines of responsibility are other important considerations.

David Firth, Chairman RNARS

Related Documents:

RNARS Computer Use & Operations

RNARS Social Media Engagement Policy

People, risks and responsibilities

Policy Scope

This policy applies to:

- The Headquarters of the RNARS
- All branches of the RNARS
- All members and volunteers of the RNARS
- All contractors, suppliers and other people working on behalf of the RNARS.

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- and any other information relating to individuals

Data Protection Risks

This policy helps to protect the RNARS from several very serious data security risks, including:

- **Breaches of confidentiality**
  For example, information being given out inappropriately

- Failing to offer choice.
  For example, all individuals should be free to choose how the RNARS uses data relating to them.

- Damage to Reputation
  For example, the RNARS could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who is a member or who works for or with the RNARS has some responsibility for ensuring data is collected, stored and handled appropriately. All those who handle personal data must ensure that it is handled and processed in keeping with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Committee is ultimately responsible for ensuring that the RNARS meets its legal obligations.
- The **Data *Protection Officer/Manager*** is responsible for the following:

❖ Keeping the Committee updated about data protection responsibilities, risks and issues.

❖ Reviewing all data protection procedures and related policies in keeping with an agreed schedule.

❖ Arranging for data protection training and advice for people covered by this policy.

❖ Handling data protection questions from members and anyone else covered by this policy.

❖ Dealing with requests from individuals to see the data that the RNARS holds about them -'subject access requests.

❖ Checking and approving any contracts or agreements with 3rd parties that may handle the RNARS's sensitive data.

- The ***IT/systems manager*** is responsible for the following:

❖ 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 3rd party services the RNARS is considering using to store or process data. For example, cloud computing services.

- The ***Marketing/Sales 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 other members to ensure marketing initiatives abide by data protection principles.

General Guidelines

- The only people able to access data covered by this policy should be those members who are authorised to do so, who ***need it for their work on behalf of the RNARS***.
- ***Data must not be shared informally***. When access to confidential information is required for the purposes of carrying out data protection principles, members working under the direction of the data protection manager can request it from the data protection manager.
- The RNARS will provide suitable awareness information to all members to help them understand their responsibilities when handling data.
- ***Members should keep all data secure*** by taking sensible precautions and by following the guidelines below as well as those guidelines used to augment this policy, e.g. *Social media engagement policy*, etc.
- 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 RNARS or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If data is no longer required it should be deleted or disposed of.
- Members should request help from the data protection manager or the Social media engagement policy manager if they are unsure about any aspect of data protection.

Data Storage

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

These guidelines also apply to data that is either stored as printed matter on paper or on other materials, and stored as electronic records that have been printed out.

Questions about storing data safely can be directed to the IT manager or to the data protection manager.

- ***When data is stored on paper*** it should be kept in a secure place beyond the reach of unauthorised people.
- Paper or files should be kept ***in a locked drawer or filing cabinet*** when not required.

- Members should ensure paper items and printouts are not left where unauthorised people can see them, e.g. when on a printer.

- ***Data printouts should be shredded*** and disposed of securely when no longer required.

Electronically Stored Data

Electronically stored data must be protected from unauthorised access, accidental deletion and from malicious activities such as hacking:

- Data should be ***protected by strong passwords*** that are regularly changed and never shared between members.

- When data is ***stored on removable media*** (CD, DVD, USB), these should be kept securely locked away 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***, and those backups tested regularly in keeping with the RNARS backup procedures.

- Data should ***never be saved directly*** to laptops or other mobile devices such as tablets or smart phones.

- All servers and computers containing data should be protected by ***approved security software and a firewall***.

Data Use

Personal data is of no value to the RNARS unless the Society can make use of it, but it is of value when data is accessed and used that is when it can be of greatest risk of loss, theft or corruption:

- When working with personal data members should ensure the ***screens of their computers*** are always locked when unattended.

- Personal data ***should not be shared informally***. In particular, it should never be sent by email as this form of communication is unsecure.

- Data must be encrypted ***before being transferred electronically***. The IT Manager/Data Protection Manager can explain how to send data to unauthorised contacts external and internal.

- Personal data should ***never be transferred outside of the EU***.

- Members should not save copies of personal data to their own computers. Always access and update the central copy of any data

Exceptions covered by these guidelines

The RNARS possesses IT systems for use in key areas:

a. Radio systems augmentation to produce data, digital and visual modes of operation.

b. Computer controlled radio repeater service connected to the internet.

c. General use computers for use as described in (a) above and also for general purpose and internet operations that include access to the RNARS website, other website services and to social media sites.

While all of these systems and the use of these systems in the RNARS HQ radio room fall under the authority of these rules and guidelines, the computer equipment used in the radio room in particular, is for general use by any authorised members, and should not contain any private or personal data or any other data pertinent to the RNARS that falls under the requirements of current legislation.

The same rules apply to members who use their own computers and removable media while working in the radio room.

Committee members who use their personal computing equipment, tablets, i-pads, smart phones, etc, which they use to manage the affairs of the RNARS must ensure that they are compliant with the requirements of the rules and guidelines of the RNARS data protection policy, and related policy documents.

The computer controlling the repeater service GB7RN is also covered by these rules and guidelines, and is under the direct responsibility and management of the Committee and its authorised specialist.

In addition, since the new generation of processor controlled radios and SDR radios can store digital information that can be transmitted and received directly or via online services, these also fall under the rules and guidelines of the RNARS because they are used to store electronic data for messaging and as such, that can mean the transmission of personal or private data, which is not allowed, except the personal data being sent by the actual operator in the normal course of radio operational traffic.

Data Accuracy

The law requires the RNARS to take reasonable steps to ensure data is kept accurate and up to date. The more important the personal data -the more important it is for the RNARS to make a greater effort to ensure that it is accurate.

It is the responsibility of all members who work with data to take reasonable steps to ensure it is kept as accurate and as up to date as possible.

- Data will be held ***in as few places as necessary***. Members should not create any unnecessary additional data sets.
- Members should ***take every opportunity to ensure data is updated***.
- The RNARS will provide ***easy access for members to update the information*** that the RNARS holds about them via its website.
- Data should be updated as soon as inaccuracies are discovered.
- It is the Marketing/sales manager's responsibility to ensure marketing databases are checked against industry suppression files every six months (?)

Subject access requests

If a member contacts the RNARS requesting information about their personal data that the RNARS holds, this is called a *'subject access request*.'

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

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

All requests from individuals should be made by email, addressed to the data protection lead at 'RNARS@mailbox.nnn' The data protection lead will respond with a standard request form, but members have the choice not to use this if known by the data lead or by a member of the Committee. The target for providing relevant data is 14 days.

The data protection lead will always have to verify the identity of anyone making a 'subject access request' before handing over any data.

Disclosing data for other reasons

Under 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 RNARS will disclose requested data. However, the data protection lead will ensure that:

- The request is legitimate
- Seek assistance from the Committee and from RNARS legal advisers where necessary

Providing information

The RNARS aims to ensure that individuals are awre that their data is being processed, and that they understand the following:

- How the data is being used
- How to exercise their rights

To these ends, the RNARS has a privacy statement setting out how data relating to individuals is used by the company.

This is available on request, but a version of this statement is also available on the Society's website.

Related Documents:

RNARS Computer Use & Operations

RNARS Social Media Engagement Policy

Acknowledgement form

Please read policy documents carefully to ensure that you understand what is required of you before signing this document.

I confirm that I have read and been informed about the content, requirements, and expectations of the following RNARS Policy Documents:

RNARS Data Protection Policy

RNARS Computer User & Operation Policy

RNARS Social Media Engagement Policy

I agree to abide by the rules and guidelines contained in each of these RNARS policies as a condition of my continuing membership of the RNARS.

I understand that if I have questions, at any time, regarding the rules and guidelines of these polices, I will consult with the social media policy manager.

I understand that when my membership of the RNARS ceases, access to the RNARS website and social media will be discontinued and all personal data will be removed.

I understand that it is my responsibility to inform the RNARS of identity theft, and that my access to RNARS online sites will be closed as a measure of protection to myself and to the Society's online operations until I have reported that I have established a new identity.

Member Signature: _____

Member Printed Name: _____

Date Joined: _____

Membership Number_____

Received By:* _____Date:_____

*To be signed off by the Data Protection Manager or by a Committee member.