South Manchester Radio and Computing Club), Also Known as South Manchester Radio Club (SMRC) Data Protection Policy

Context and overview

Key details

* Policy prepared by: Mr. D Crowe
* Approved by board / management on: 01/03/2024
* Policy became operational on: 14/03/2024
* Next review date: Every 12 months from becoming operational.

Introduction

SMRCC/SMRC needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Clubs data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures SMRCC/SMRC:

* Complies with data protection law and follow good practice
* Protects the rights of Members, volunteers, customers and partners
* Is open about how it stores and processes individuals' data
* Protects itself from the risks of a data breach

Data protection law

General Data Protection Regulation 2018 (As of May 2018) describes how organizations — including SMRCC/SMRC— 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/Regulation is underpinned by eight important principles. These 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 the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

* The Clubs Headquarters of SMRCC/SMRC
* All Committee Members, Members and volunteers of SMRCC/SMRC
* All contractors, suppliers and other people working on behalf of SMRCC/SMRC

It applies to all data that the Club holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018 (As of May 2018). This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* Plus any other information relating to individuals to support their membership

Data protection risks

This policy helps to protect SMRCC/SMRC from some very real data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Failing to offer choice**. For instance, all individuals should be free to choose how the Club uses data relating to them.
* **Reputational damage.** For instance, the Club could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who Members and volunteers for or with SMRCC/SMRC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each Committee Members, Members or Volunteer that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

* The Committee Members are ultimately responsible for ensuring that SMRCC/SMRC meets its legal obligations.
* The Committee Members are responsible for:

o Keeping all Members and Volunteers updated about data protection responsibilities, risks and issues.
o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
o Arranging data protection training and advice for the people covered by this policy.
o Handling data protection questions from volunteer and anyone else covered by this policy.
o Dealing with requests from individuals to see the data SMRCC/SMRC holds about them (also called 'subject access requests').
o Checking and approving any contracts or agreements with third parties that may handle the Clubs sensitive data.

* The Committee Members are responsible for:
o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
o Performing regular checks and scans to ensure security hardware and software is functioning properly.
o Evaluating any third-party services the Club is considering using to store or process data. For instance, cloud computing services.

* The Committee Members are responsible for:
o Approving any data protection statements attached to communications such as emails and letters.
o Addressing any data protection queries from journalists or media outlets like newspapers.
o Where necessary, working with other members and volunteer to ensure marketing initiatives abide by data protection principles.

General volunteer 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**. When access to confidential information is required, Members and volunteers can request it from a Committee Member.
- **SMRCC/SMRC will provide training** to all Committee Members, Members and volunteers to help them understand their responsibilities when handling data.
- Committee Members, Members and volunteers should keep all data 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 unauthorized people**, either within the Club 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.

* Members and Volunteers should request help from a Committee Member if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Committee Member.

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet.**
- Trustees and volunteers should make sure paper and printouts are **not left where unauthorized people could see them**, like 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 unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable 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 an 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 Club standard backup procedures.
- 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 SMRCC/SMRC unless the Association can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, Committee Members, Members and volunteers should ensure the screens of their computers are always 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. Unless in an encrypted attached file.

- Sensitive Data should be encrypted before being transferred electronically.

- Personal data should never be transferred outside of the European Economic Area.

- Committee Members, Members and volunteers should not save copies of personal data to unauthorized computers. Always access and update the central copy of any data.

Data accuracy

The law requires SMRCC/SMRC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort SMRCC/SMRC should put into ensuring its accuracy.

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

- Data will be held in as few places as necessary. Committee Members, Members and volunteers should not create any unnecessary additional data sets.

- Committee Members, Members and volunteer should take every opportunity to ensure data is updated. For instance, by confirming a member's details when they contact the association when appropriate.

- SMRCC/SMRC will make it easy for data subjects to update the information SMRCC/SMRC holds about them. For instance, via the Club website.

- Data should be updated as inaccuracies are discovered. For instance, if a member 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 SMRCC/SMRC are entitled to:

* Ask what information the Club 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 Club is meeting its data protection obligations.

If an individual contacts the Club requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Secretary at Secretary@smrcc.com. The Secretary can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £0 per subject access request. The Secretary will aim to provide the relevant data within 30 days.

The Secretary will always verify the identity of anyone making a subject access request before handing over any information.

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, SMRCC/SMRC will disclose requested data. However, the Secretary will ensure the request is legitimate, seeking assistance from the Committee Members and/or from legal advisers where necessary.

Providing information

SMRCC/SMRC aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

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

[This is available on request. A version of this statement is also available on the Club website.]