



## Data Protection Policy

### **Scope**

Rochdale AFC is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the General Data Protection Regulation (GDPR) and related data protection laws. We recognise that the correct and lawful treatment of personal data will maintain confidence in Rochdale AFC and will support Rochdale AFC to meet its commercial objectives.

The GDPR relates to 'data controllers' and 'data processors'. A data controller determines the purpose and means of the processing of personal data; they are responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data, including sensitive information (known as "special category" data under the GDPR), which we collect about participants as part of the programmes we deliver.

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. It is the personal responsibility of all employees (temporary or permanent), Directors, contractors, agents and anyone else processing data, or who has access to personal or sensitive information on our behalf, to comply with this Policy. For the purpose of this Policy, the above will be referred to as 'employees.'

This Policy continues to apply to employees and individuals, even after their relationship with Rochdale AFC ends. Any breach of this Policy may result in disciplinary action.

### **Introduction**

In order to operate efficiently, Rochdale AFC needs to collect and use information about people with whom it works as well as customers and fans. These may include members of the public, current, past and prospective employees, sponsors, clients, fans and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central Government.

This Policy covers all personal data, however they are held, on paper or in electronic format, and the rights of individuals (data subjects) who wish to see information Rochdale AFC holds about them.

Everyone managing and handling personal information needs to understand their responsibilities in complying with the GDPR. It is a legal requirement that Rochdale AFC complies with the GDPR, and all members of staff have a responsibility to ensure Rochdale AFC's legal compliance.

This Policy is intended to facilitate compliance and all staff should be aware of its content and the key requirements of the GDPR. Rochdale AFC's Staff handbook also refers to staff obligations with regard to Data Protection and managers should ensure that staff are provided with the appropriate knowledge and training to ensure they can fulfil their responsibilities.

All relevant documents relating to the Data Protection legislation are available on the intranet and Rochdale AFC's Data Protection Officer (DPO) is responsible for making staff aware of these documents. The DPO for Rochdale AFC is COO George Delves, who can be contacted on 01706 644648 or in writing at Rochdale AFC, Crown Oil Arena, Sandy Lane, Rochdale, OL11 5DR.

## **Responsibilities**

Rochdale AFC Directors will have responsibility for compliance of Rochdale AFC with the GDPR and related data protection laws and regulations.

Whilst Rochdale AFC's Board is ultimately responsible, both personal and corporate responsibility applies. All employees are therefore responsible for ensuring compliance with the Principles of the GDPR by complying with this Policy.

Line managers must ensure that those staff managing and handling personal information are adequately trained and supervised with regard to the requirements of this Policy. Please contact Rochdale AFC's DPO to discuss your training requirements.

## **Definitions**

- Data is information, which is stored electronically, on a computer, or in certain paper-based filing systems.
- Data subjects means an identified or identifiable natural person.
- Personal data means any information relating to an identified or identifiable natural person ('data subject').
- Data controllers are the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; they are responsible for establishing practices and policies in line with the GDPR.
- Data Subject is an identified or identifiable natural person.
- Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection Policy and any applicable data security procedures at all times.
- Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of Rochdale AFC.
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise.
- Special category of personal data means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and

the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This type of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned (sensitive personal data).

## **The Principles of the GDPR**

The principles which form the basis of GDPR state that data must be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- Accurate and where necessary kept up to date (Accuracy)
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

## **Lawfulness, Fairness, Transparency and Consent**

- The GDPR is not intended 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 GDPR allows Processing for specific purposes, some of which are set out below:
  - The Data Subject has given his or her Consent;
  - The Processing is necessary for the performance of a contract with the Data Subject;
  - To meet our legal compliance obligations;
  - To protect the Data Subject's vital interests;
  - To pursue our legitimate interests.

When sensitive personal data is being processed (now known as "special categories of personal data" under the GDPR), additional conditions must be met. When we process sensitive personal data, we will ensure compliance with these requirements.

## **How We Obtain Consent**

Under the GDPR, a higher standard is required when it comes to obtaining consent. We have therefore updated our procedure to take account of this requirement. Where there is no other lawful ground for processing, we will obtain your consent. We will not seek consent for use of crowd based images for example on a match day.

- Be consent, we mean that you have a genuine choice. We will never make it a pre-condition of our products and services that you must provide consent. We will never assume your consent and always obtain your specific agreement first.
- We will maintain records of the consents that you provide to us, however, you are

able to withdraw your consent at any time by writing to us at Rochdale AFC, Crown Oil Arena, Sandy Lane, Rochdale, OL11 5DR.

### **Purpose Limitation**

We will only collect and process personal data for specified explicit and legitimate reasons. We will not further process that personal data unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

### **Data Minimisation**

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

### **Accuracy**

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 ensure that personal information that is inaccurate is either erased or rectified without delay.

### **Storage Limitation**

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

### **Security Integrity and Confidentiality**

We will implement appropriate technical and organisational measures to guard against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and activities, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks.

Employees are required under this Policy to support Rochdale AFC in meeting its obligations under the GDPR and related regulations to maintain confidentiality. In doing so, employees must use secure passwords on the systems that they are required to use as part of their roles. Passwords must contain a minimum of 7 characters and must contain at least 3 of the following characteristics:

- Latin uppercase letters (A through Z)
- Latin lowercase letters (a through z)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters such as: exclamation point (!), dollar sign (\$), number sign (#), or percent (%).

- Must not share their passwords with anyone else.
- Must take care when sending emails to ensure that they are sent only to the intended recipients.
- When processing 'sensitive information', this should be done by secure means such as password protecting documents or secure.
- Must lock computers when not attended to avoid unauthorised access.
- Filing cabinets containing personal data must be locked outside of normal working hours and keys must be held securely by nominated staff.
- Ensure that electronic data is stored in secure server areas, not on computer hard drives, laptops or other mobile devices.
- Must not use personal email addresses to conduct Club business.
- Any electronic data backed up to media such as CD must be kept physically secure.
- If any data are to be taken from the office (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location they are being held. In particular data must be protected from unauthorised access.

To avoid unauthorised access to personal information, Rochdale AFC will implement appropriate security controls as follows:-

### **Building Access**

All visitors will be required to identify themselves on arrival with appropriate identification and sign a signing in book. This must confirm the name of the visitor, time of arrival and exit, who they represent and who they are visiting.

### **Security Pass**

All visitors must display a visitor pass at all times so employees are aware of their status as a visitor. Any visitor not displaying a visitor pass must be challenged immediately.

### **Secure areas**

Visitors must not be given access to secure areas, unless necessary to perform their task, and must not be left unattended.

### **Training**

The DPO will arrange appropriate data protection training to take place with all staff on annual basis if possible but at least every two years. This training will include IT security and the data protection laws in place at the time.

### **Sharing Information with Third Parties**

It may be necessary for Rochdale AFC to share information with third parties as necessary for meeting the objectives of Rochdale AFC. In doing so, the GDPR requires us to ensure that we receive sufficient guarantees that these providers will implement appropriate security and technical measures to protect the confidentiality of information which they have access to.

Rochdale AFC will therefore only share the Personal Data with third parties in the following circumstances:

- They have a need to know the information for the purposes of providing the contracted services.
- Provide satisfactory evidence of the security and controls that they have implemented to maintain the confidentiality of the personal information that they will have access to and the procedures they have in place for sharing information e.g. encryption, secure email, password protection.
- Sharing the Personal Data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained.
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.
- Rochdale AFC uses the services of a third-party IT service provider. In providing remote support, it is necessary for them to access Trust systems, such as the server or email accounts. This may be necessary, for example, to correct a system fault or other IT issue which may arise. In doing so, we will ensure that our third-party service provider has signed a fully executed agreement which accords with the GDPR, including details of how their own systems provide appropriate security, and how their own staff will maintain confidentiality.

When Rochdale AFC shares information with third parties, it will implement and use appropriate methods of secure transfer to prevent the occurrence of a data breach. It is critical that staff adopt these working practices. When documents containing personal information are transferred to third parties, they should be sent using password protected documents. The password should not be sent by email to the third party. You should contact the third party directly to provide the password for security purposes.

Where the large volumes of personal information are to be transferred to a third party, this should be done using a secure method of transfer such as WeTransfer or any other form of transferring personal information as directed by management.

### **Data Subjects Rights and Requests for Information**

Data Subjects have additional rights under the GDPR when it comes to how we handle their Personal Data. These include rights to

- Withdraw Consent to Processing at any time.
- Receive certain information about the Data Controller's Processing activities.
- Request access to their Personal Data that we hold.
- Prevent our use of their Personal Data for direct marketing purposes.
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data.
- Restrict Processing in specific circumstances.
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest.

- Object to decisions based solely on automated processing, including profiling (ADM).
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

### **Procedure for subject access requests**

Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward this DPO immediately.

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

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- 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.
- Our employees will refer a request to the DPO for assistance in difficult situations.

Employees should not be pressured into disclosing personal information.

On receipt of a subject access request, we will send a letter to the requester acknowledging receipt.

- We will respond to subject access requests as soon as possible, but in any event no later than 1 month from the receipt of the request subject
- If the nature of the request is complex, or there are other legitimate reasons for doing so, we may, if necessary, extend the period for up to 2 months. If we require an extension of time of over 1 month to deal with a subject access request, we will inform the requester as soon as possible, but in any event no later than 1 month from the date that the request was made.

We will not charge a fee for responding to subject access requests unless the request, in the opinion of Rochdale AFC, is unfounded, excessive and/o repetitive.

### **How we will we notify Data Subjects about how we use their Information.**

As part of our obligations to process information lawfully and fairly, we must ensure under the GDPR that this is also done transparently. We are therefore required to notify data subjects about the following matters:

What information we process about them:

- The purpose of the processing.
- The legal basis for the processing.
- Who we may share information with.
- How long we hold it for.
- What their individual's rights are.
- How a Complaint may be made.

Rochdale AFC will meet this requirement by preparing and communicating privacy notices and make them available in hard copy and on the website.

**Transfer of Data**

Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states, Iceland, Norway and Liechtenstein) unless the country they are being transferred to has the same or equivalent standards of Data Protection. This has implications for data placed on the Internet and use of e-mail where servers are based abroad.

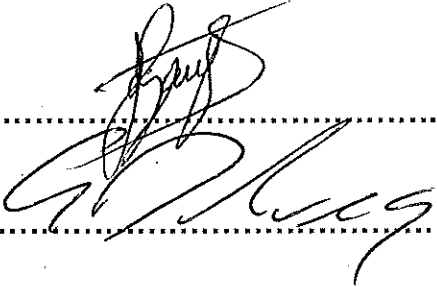
If information is required to be transferred abroad then checks must be made to ensure that the data are held securely during transfer and that data recipients apply data protection rules equivalent to those under the GDPR. Advice on this should be sought from Rochdale AFC's DPO.

**Change to Policy**

We reserve the right to change this Policy at any time and notification of any changes will be communicated accordingly. The policy will be reviewed annually and audited annually 6 months from the review date.

**Approval**

Signed: Simon Gauge..... Chairman/RAFC  
(On behalf of the board)



Signed: George Delves ..... DPO/RAFC

Version date: 10 Mar 2023  
New review date: 31 Mar 2024