



## **Bristol Rovers Community Trust Data Protection Policy & Privacy Notice**

<b>Approved By</b>	<b>Version</b>	<b>Issue date</b>	<b>Review date</b>	<b>Contact person / role</b>
Board	3	Dec 2025	Dec 2028	Community Operations Manager

NB: Board Review must consider:

- Changes to the Trust services and activities
- Any changes to the legislative framework
- Any new guidance published by the ICO which is applicable to the Trust

### **Data Protection Officer Details**

Name	Nathan Hallett-Young
Job Title	Community Operations Manager / Data Protection Officer
Telephone	0117 9522581
Email	info@bristolroverscommunity.org.uk
Postal Address	The Memorial Stadium, Filton Avenue, Bristol BS7 0BF

### **Introduction**

This policy is written in accordance with the Data Protection Act, General Data Protection Regulation (GDPR) and any other relevant legislation. Bristol Rovers Community Trust (BRCT) is registered under the Act as a Data Controller under number ZA124301.

### **Statement**

In accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) (EU) 2016, BRCT will meet its legal obligations concerning confidentiality and the data security standards by having the appropriate physical and technical measures in place to ensure the security of any data collected, contained or handled by its systems, employees and any third parties. Access to BRCT's systems and information by all staff, contractors, subcontractors, suppliers, is diligently monitored with the appropriate pre- security checks including contractual agreements





that sets out the minimum security requirements for confidentiality, integrity, availability and accountability of BRCT's information and systems.

Protective measures in place for the secure transfer of personal data to and from a 3rd party includes, secure email, password protection, and anonymization if applicable. Our purpose for holding personal data and whom we share it with, including the security controls in place to protect the data are outlined in this policy and Privacy Notice.

The Data Protection Act and GDPR help to protect personal data and place restrictions on BRCT's ability to disclose personal data within the UK and overseas.

### **Purpose**

The purpose of this policy is to set out BRCT's commitment and procedures for protecting personal data, and individual rights and obligations in relation to personal data. BRCT regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

This policy applies to the personal data that is collected and processed for employees, job applicants, participants who attend programmes and courses, contractors, partners and other individuals to carry out its business and organisational functions.

### **Definitions**

Personal data is any information that can be used to identify an individual, for example, information such as name, date of birth, email address, postal address, telephone number, etc. It also applies to data held in photographs or video clips (including CCTV). It includes data held on in any system or format, electronic or manual.

Special categories of personal data is any information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal records data is any information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Processing includes obtaining, recording, organising, using, disclosing, deleting, and simply holding data so therefore in practice, anything done with data will amount to processing.

BRCT may collect personal information when you register on BRCT programmes or activities, pay for courses, request information, make a donation, subscribe to Newsletter or otherwise provide BRCT with personal information.





**BRCT is committed to processing personal data in accordance with the following Data Protection Principles:**

- Personal data is processed fairly, lawfully and in a transparent manner
- Personal data is obtained only for specified, explicit and legitimate purposes
- Personal data that is collected for the purpose of processing is adequate, relevant and limited to what is necessary
- Personal data is accurate and all reasonable steps will be taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is not to be kept for longer than is necessary for the purpose of processing
- Personal data is kept secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

Data subjects will be clearly informed of the reasons for processing their personal data, how such data will be used and the legal basis for processing. Personal data of individuals will not be processed for other reasons

**BRCT will:**

- Inform individuals why personal information is needed and how it will be used
- Only share personal information with consent from the individual, or when it is necessary and legally appropriate to do so
- Ensure when information including electronic or paper format is authorised for disposal, it is done appropriately and securely
- Ensure appropriate security measures are in place to safeguard personal information by adopting best practice e.g. strong password protection, secure networks, secure buildings where information in all formats is stored (please refer to BRCT IT Security Policy)
- Respond to requests for access to personal information in line with the Data Protection Act and the GDPR
- Train staff so that they are aware of their responsibilities and of BRCT's relevant policies and procedures.
- BRCT will use Data Protection Impact Assessment (DPIA) as a process to help identify and minimise the data protection risks of a project / activity.

**Special Categories of Personal Data**

Special category data is subject to stricter conditions for processing under the GDPR. As such, measures will be taken to ensure that special category data is handled appropriately.

Special category data can only be processed if it meets one of several conditions in addition to the conditions outlined above:

- explicit consent of the individual (that will be kept on file)
- contractual obligations of an individual or compliance with employment law





- processing in the vital interests of the individual (where the individual cannot give consent or it cannot reasonably be obtained) or another person, where the individual has unreasonably withheld consent;
- the data is necessary for medical purposes and processing is done by a health professional or someone subject to an equivalent duty of confidentiality
- processing for the monitoring of equality of opportunity;

## Types Personal Data Obtained, Controlled and Processed

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, age, date of birth and gender.
- Contact Data includes billing address, delivery address, email address and telephone numbers, email address.
- Financial Data includes bank account and payment card details.
- Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us.
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- Profile Data includes your username and password, purchases or orders made by you, your interests, occupation, preferences, feedback and survey responses.
- Usage Data includes information about how you use our website, products and services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- Medical information includes disability, allergies and any/or accidents and incidents whilst in our care.
- Race and Ethnicity
- Religious beliefs

## How Personal Data is Used

We use information held about you in the following ways:





- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.
- To create a membership profile for you to help us provide a more personalised service which is suited to meet your preferences
- To ensure that content from our web site is presented in the most effective manner for you and for your computer
- To send you our newsletters or catalogues or provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes
- To carry out our obligations arising from any contracts entered into between you and us
- To allow you to participate in interactive features of our service, when you choose to do so
- To notify you about changes to our service.

## Accuracy and Updating of Personal Data

The law requires Bristol Rovers Community Trust 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 the charity should put into ensuring its accuracy.

It is the responsibility of all employees 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. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- Bristol Rovers Community Trust will make it easy for data subjects to update the information the charity holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

## Retention of Personal Data





We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data. In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

## Confidentiality and Privacy

All BRCT Staff must take appropriate action to protect the confidentiality and integrity of all personal data from the point of collection and point of destruction. In this context;

- Confidentiality means only people who are authorised to know and use personal data can access it
- Integrity mean that personal data is accurate and suitable for the purpose for which it is processed

BRCT treats all personal information as confidential however; confidentiality may be broken in exceptional circumstances:

- When there is a serious risk of harm or abuse to an individual or someone else
- To protect others, for example, information about possible child abuse should be disclosed to the appropriate agency
- To prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.

## Security

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer.





When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.

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

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people cannot access them.
- 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 and never shared between employees.
- If data is stored on a removable storage device, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- 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 charity's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

## Consent

BRCT will never sell personal information to third parties or share information without consent that will be held on file. You will be given an option to “opt-in” if you wish to receive further communication or information from BRCT or Bristol Rovers Football Club. You will be able to select preferred method of communication:- Email, Telephone, SMS or mail. Electronic communications will always give you the option to unsubscribe or you can request this by telephone or in writing.

## Transfer of Personal Data to Third Parties

Protective measures in place for the secure transfer of personal data to and from a 3rd party includes, secure email, password protection, and anonymization if applicable. Our purpose for holding personal data and whom we share it with, including the





security controls in place to protect the data are outlined in this policy and Privacy Notice.

## Training of Staff and Volunteer's

BRCT staff will as a minimum training requirement complete certificated Data Protection and Information Sharing and Processing modules and annual refresher training. Those individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them. All BRCT staff are responsible for making informed decisions to protect and properly manage personal data. BRCT staff are responsible for ensuring that they are aware and understand the requirements of the Policy and for ensuring compliance on a day-to-day basis. Failure to comply with this and related policies may result in Disciplinary action.

BRCT acknowledge that information is a valuable asset and will ensure that the information it holds, in whatever form, is appropriately managed and stored to protect the interests of individuals and stakeholders.

Volunteers will have the opportunity to attend relevant training if deemed appropriate o

