COMMUNITY TRUST

DATA SECURITY POLICY

Policy Updated: 24/05/2018

Next Update due: 24/05/2019

1. Introduction

Blackburn Rovers Community Trust (BRCT) needs to collect and use certain types of information about the individuals or service users who come into contact with BRCT in order to carry on our work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998.

2. Data Controller

BRCT is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

BRCT may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The individual/service user will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows BRCT to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty

b) Protecting vital interests of a individual/service user or other person

c) The individual/service user has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the individual/service user's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

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.

BRCT intends to ensure that personal information is treated lawfully and correctly.

To this end, BRCT will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes;

c) Shall be adequate, relevant and not excessive in relation to those purpose(s);

d) Shall be accurate and, where necessary, kept up to date;

e) Shall not be kept for longer than is necessary;

f) Shall be processed in accordance with the rights of data subjects under the Act;

g) Shall be kept secure by the Data Protection Officer who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information;

BRCT will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken;
    - The right of access to one's personal information;
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information).
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when

- An individual/service user clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

BRCT will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, BRCT will ensure that the individual/service user:

a) Clearly understands why the information is needed;

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing;

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress;

e) Has received sufficient information on why their data is needed and how it will be used;

f) Understands that BRCT may act considering legitimate interests using the following three-fold steps:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

5. Data Storage

Physical (office security)

Staff members should only have access to data that is specifically relevant to their role.

BRCT operate a 'clean desk policy' – see separate document.

All offices are secured by mag-locks and/or digit locks (with only specific staff having access to certain areas).

All sites BRCT manage are covered by alarm systems, CCTV and on-site security is available at the stadium/BRIC.

Any form of printed data should be held within a locked cabinet then destroyed once uploaded onto the computer system. Physical copies of data should be held for no longer than one year in length (a time frame we are working to reduce further).

Information and records relating to service users will be stored securely and will only be accessible to relevant authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of safely and appropriately.

IT

BRCT have opted for a cloud-based data storage solution (Onedrive) within Office 365 – which is fully GDPR compliant. Office 365 also offers an encrypted email offer amongst other data security elements. Staff members should only have access to data that is specifically relevant to their role.

Staff members should only have access (using permissions) to shared areas that are specifically relevant to their role.

All staff and guests at BRCT have unique logins and sign-up to an e-safety policy which advises best practise when using the network, technological devices and the internet.

BRCT have opted for a customer-facing booking system called 'Open Play' which is a cloud based encrypted solution.

BRCT have opted for a 'follow-me' printer system which has 'Papercut' software meaning staff and participants alike must log-in at the printer for printouts.

BRCT have ensured all hardware and software is current (has support from creators); with a continuous challenge to bring all IT infrastructure into its most current format.

BRCT have a single internet feed with separate access from BRFC and other site users.

BRCT will ensure they have adequate software to safeguard against external parties accessing the network and thus data.

BRCT have ensured they have encrypted remote access into the network.

It is BRCT's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Third parties utilising on site IT will have restricted access through a guest user area or guest wi-fi. They will have no access to any personal information.

Authorised staff have access to all relevant online data recording and monitoring systems. These systems are regularly backed up using secure exported spreadsheets and stored for an appropriate period of time in which they are likely to be used. Following this period all data will be destroyed.

6. Data access and accuracy

All individuals/service users have the right to access the information BRCT holds about them. BRCT will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, BRCT will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- Everyone processing personal information is appropriately trained to do so;
- Everyone processing personal information is appropriately supervised;
- Anybody wanting to make enquiries about handling personal information knows what to do;
- It deals promptly and courteously with any enquiries about handling personal information;
- It describes clearly how it handles personal information;
- It will regularly review and audit the ways it hold, manage and use personal information;
- It regularly assesses and evaluates its methods and performance in relation to handling personal information;
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

7. Data Disposal

- It is BRCT's responsibility to ensure that any form of data following its retention period (as identified in the Data Protection Policy) is disposed and destroyed safely.
- All physical copies of data should be safely disposed via confidential shredding.
- It is BRCT's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

This document has been approved by the board of trustees

Name: George R Root (Chair of Trustees)