DATA PROTECTION POLICY

INTRODUCTION

1 The Trust may have to collect and use information about people with whom we work. These may include members and suppliers. This personal information must be handled and dealt with properly (however it is collected, recorded and used) whether it be on paper or computer records. There are safeguards within the Data Protection Act 1998 to ensure this.

2 We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we serve. We will ensure that we treat personal information lawfully and correctly.

3 To this end we fully endorse and adhere to the Principles of Data Protection as set out in the Data Protection Act 1998.

The principles of data protection

4 The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

5 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 specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
c. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
d. shall be accurate and where necessary, kept up to date;
e. shall not be kept for longer than is necessary for that purpose or those purposes;
f. shall be processed in accordance with the rights of data subjects under the Act;
g. shall be kept secure i.e. protected by an appropriate degree of security;
h. shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

6 The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **“sensitive” personal data**.

7 Personal data is defined as data relating to a living individual who can be identified from:

a. that data;
b. that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

8 Sensitive personal data is defined as personal data consisting of information as to:
   a. racial or ethnic origin;
   b. religion or other beliefs;
   c. trade union membership;
   d. physical or mental health or condition;
   e. sexual life;
   f. criminal proceedings or convictions.

Handling of personal/sensitive information

9 We will, through appropriate management and the use of strict criteria and controls:
   a. observe fully conditions regarding the fair collection and use of personal information;
   b. meet our legal obligations to specify the purpose for which information is used;
   c. collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
   d. ensure the quality of information used;
   e. apply strict checks to determine the length of time information is held;
   f. shall be accurate and where necessary, kept up to date;
   g. shall not be kept for longer than is necessary for that purpose or those purposes;
   h. shall be processed in accordance with the rights of data subjects under the Act;
   i. shall be kept secure i.e. protected by an appropriate degree of security;

10 In addition, we will ensure that:
   a. everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
   b. methods of handling personal information are regularly assessed and evaluated;

11 All Board members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

12 All Board members must take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:
   a. paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
   b. personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
   c. individual passwords should be such that they are not easily compromised.

13 All contractors, consultants, partners or Directors must:
   a. ensure that they and all of their staff who have access to personal data held or processed for or on behalf of us, are aware of this policy and are fully aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract

between the Company and that individual, company, partner or firm;

b. allow data protection audits by us of data held on our behalf (if requested);
c. indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

14 All contractors who are users of personal information supplied by us will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

Notification

15 The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

DATA RECORDS MANAGEMENT

16 The main objective of the section is to turn the above policy into practical records management. There are three issues highlighted:

a. **Accountability** –adequate records will be maintained to account fully and transparently all actions and decisions;
b. **Security** – records will be secure from unauthorised or inadvertent alteration or deletion. Records will be held in a robust format which remains readable and accessible for as long as information is relevant and/or required;
c. **Records Retention and disposal**

Accountability - Roles and Responsibilities

17 The following roles have been designated within the Trust:

a. David Allen: Data controller—the person responsible for deciding how and why personal data is to be processed
b. Andy Baker: Data processor—the person tasked with carrying out data processing on behalf of the controller
c. Huw Jones: Data Protection Officer – the person responsible for ensuring that the Trust is compliant with Data Protection laws.

18 All breaches of data protection must be reported to the Data Protection Officer who will, following investigation, report the matter to the Board.

Security

19 We take a number of steps to ensure that both members' and the Board's data is protected:

a. we take steps to minimise the risk of cybercrime through the purchase of a certificate for the domain so all traffic is encrypted;
b. ensure access to the database is strictly restricted to the minimum number of individuals required to manipulate data;
c. we provide the Board with regular training on all relevant policies and procedures;

d. our terms and conditions include what members need to know about our use of their data, including the purposes for which it is collected, and their rights.

Records Creation and Disposal

20 We hold the following personal data on our current and past members:
   a. Member name and address;
   b. Date of Birth (for voting purposes at AGMs);
   c. Contact details: phone and email;
   d. Whether the member is a shareholder or not in Cardiff Blues Ltd.

21 We will not retain information on any individual who is no longer holds a member of the Trust than 3 years after their membership has expired.

Review

22 This policy will be reviewed annually or at any time any that National Guidance is amended.