BWFCST DATA PROTECTION POLICY

1.0 Introduction

1.1 This policy has been produced by the Bolton Wanderers Supporters Society Limited (hereafter referred to as BWFCST or "the Trust"), adopted at its Steering Group Meeting held on 16 April 2016.

1.2 The Data Protection Act 1998 (hereafter referred to as DPA 98) is founded on a perceived need for privacy in the context of the use by the BWFCST of individuals' personal data. The Trust processes personal data in respect of members and occasionally third parties; these are the data subjects. The law outlines a set of rights for data subjects, which are exercisable against both the data controller and any data user who may cause data to be inappropriately or unlawfully disclosed. Consequently, the Trust is subject to the provisions of the DPA 98.

2.0 Notification

2.1 The BWFCST is a 'Not for Profit' organisation and, as such, is not required to register with the Information Commissioner's Office. Should the status of the Trust change, the data controllers will ensure that the registrable particulars are included in the Information Commissioner's Public Register. The registrable particulars are:

- the data controller's name and address
- a description of the personal data being, or to be, processed and the category of data subjects to which they relate
- a description of the purpose of processing
- a description of the intended recipients of the data
- a list of the countries outside the European Economic Area that will or might be in receipt of the data

3.0 Purposes

3.1 The BWFCST processes personal data (and occasionally sensitive personal data) for the purposes of:

- administration of membership records
- processing for "Not for Profit" organisations
- fundraising in support of the aims and objectives of the trust
- staff administration (in the event of the trust employing staff)

4.0 Roles and Responsibilities

4.1 The Trust board determines the purposes for which and the manner in which any personal data are, or are to be, processed. Consequently, the Trust board members are designated as "data controllers". The data controllers will appoint a board member to act as the Data Protection Officer (DPO) who will be responsible for the application of these Data Protection rules in accordance with current Data Protection legislation.

4.2 All board members and other persons that process personal data on behalf of the board are to comply with the legislation.

4.3 The Trust Secretary is to maintain and retain a register of members. This register is to be in electronic format and will therefore be subject to the requirements of the DPA 98. Thereafter,

access to the register (or copies of the register) is limited to those performing a lawful purpose on behalf of the Trust board.

5.0 Processing Personal Data

5.1 The definition of processing is wide and involves, the act of obtaining, recording or holding Personal Data or carrying out any operation on that Personal Data, including:

- organisation, adaptation or alteration of the data
- retrieval, consultation, monitoring or use of the data
- disclosure of the data by transmission, dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the data

6.0 Member and Third Party Data

6.1 Member personal data, which may be provided electronically or manually, is processed by the Trust and stored in an electronic register. Once it is processed (stored) on Trust equipment, it becomes subject to the DPA 98 and thereafter is to be processed (handled and protected) accordingly.

6.2 Third party data may be provided by members or others. Where the trust has access to third party data it shall protect it to the same standards as all other personal data held by the Trust.

7.0 Fair Collection Notice

7.1 Any document, whether manual or web based, which seeks to gain personal data is to contain a 'Fair Collection Notice', which includes:

- the identity of the data controllers
- the purpose or purposes for which the data are intended to be processed
- any other information that is necessary to enable the processing to be fair

8.0 Codes of Practice – Member & Third Party Personal Data

8.1 The Data Protection Principles form the backbone of the legislation as they lay out the obligations with which data controllers must comply when processing personal data. The following codes of practice are generic, link to those principles and outline how the data controllers will meet those obligations.

9.0 Fair and Lawful Processing

9.1 Those processing personal data on behalf of the data controllers are to ensure that:

- the data has been obtained openly and that the person from whom it has been obtained has not been misled or deceived as to the purpose for which the data was required
- the data has been obtained from a person who is either authorised to provide it or required to provide it by other legislation or convention applicable in the UK
- when the data subject provides the data, he is provided with detail about the identity of the data controller and the purpose for which the data will be used
- they comply with at least one of the following conditions when processing personal data:
  - the data subject has given his express or implied consent
  - the processing is necessary for the performance of a contract to which the data subject is party
  - the processing is necessary in order to comply with some legal obligation
  - the processing is necessary to protect the vital interests of the data subject
  - the processing is necessary for the administration of justice
  - the processing is necessary for the legitimate interests of the data controllers

and

Although the trust does not routinely process sensitive personal data, should it be necessary to do so, at least one of the following conditions must also be met:

- the data subject has given his express consent
- the data controller is obliged by law to process information in relation to employment
- the processing is necessary to protect the vital interests of the data subject or another
- the processing is carried out in the course of legitimate activities of any body or organisation, which is not established or conducted for profit, and exists for political, philosophical religious or trade union purposes
- the data subject has already made the data public
- the data is required in relation to legal proceedings
- the processing is necessary for the administration of justice
- the processing is necessary for medical purposes
- the processing is related to racial or ethnic origin and is necessary to prevent inequality or abuse

10.0 **Data Quality**

10.1 Personal data relating to members are to be:

- obtained only for the purposes of the Trust
- adequate, relevant and not excessive for the pursuance of those purposes
- accurate and kept up to date
- those processing personal data are to ensure that the data subject is aware that the onus rests with them to update personal data

11.0 **Data Retention**

11.1 Member data is to be retained whilst ever the subject remains a member of the Trust. Once an individual ceases to be a member, personal data is not to be disclosed to any third party unless such disclosure is lawful.

12.0 **Data Review**

12.1 Personal data relating to previous members are to be kept separate from data relating to current members. This is to ensure such data is properly processed. Such data is to be retained for a period of 12 months. If after 12 months membership is not renewed, data is to be anonymised so that it is no longer subject to the DPA 98. The only detail to be retained is the member's name, date of joining, date of leaving and member number.

13.0 **Disclosure**

13.1 Those persons with access to the personal data, who process the data on behalf of the data controllers, are to ensure that:

- the disclosure of personal data is lawful and in accordance with the rights of data subjects as outlined in this document
    - only such data is to be disclosed in order to achieve the purpose (eg data passed to Bolton Wanderers Development Association for the issue of Lifeline or Goldline redeemable vouchers would only require member's name and member card number in order for BWDA to issue the vouchers. However if the trust is not in possession of the Lifeline/Goldline member card number, additional data would need to be passed to enable the proper identification of the data subject)
- they do not knowingly or recklessly disclose personal data or any information contained in personal data relating to data subjects unless they do so in accordance with the purposes of the data controllers and on behalf of the data controllers
- they do not sell or offer to sell personal data relating to members or third parties

14.0 **Security**

14.1 The data controllers are to ensure that technical measures exist to protect members' personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage.

14.2 A duplicate register is to be maintained by the Trust Secretary. Access to the personal data is to be controlled and limited to those who need access for the performance of their duties.

15.0 **Rights of Data Subjects**

15.1 The DPA 98 contains a set of rights for data subjects, the majority of which are exercisable against the data controllers. The following paragraphs outline the basic rights of individuals. However, it should be noted that those rights are subject to exemptions that have been enacted for the benefit of data controllers.

15.2 Right of Access to Personal Data.

Persons are entitled to be told whether the trust, or someone else on its behalf, is processing their Personal Data. Requests for access to personal data are to be submitted to the DPO in accordance with Appendix A.

15.3 Right to Prevent Processing Causing Damage or Distress.

If a data subject believes that the trust is processing Personal Data about him/herself in a way that causes, or is likely to cause, substantial unwarranted damage, or substantial unwarranted distress, to him/her or to anyone else, the data subject may ask the trust to stop processing the data concerned. The request must be made in writing to the data controllers and must specify why the processing is or will cause substantial damage or substantial distress. The DPO will investigate the claim on behalf of the data controllers and will provide the data controllers with a draft written response enabling them to respond within 21 days. The response will either:

- confirm compliance or an intention to comply with the data subject's request, or
- advise that the data controllers consider that part or all of the request is unjustified and the extent to which they have complied or intend to comply with it

Where a data subject considers that the data controllers have failed to comply (in full or in part) with a valid request, he or she may apply to the court for an order for compliance. Assistance can be obtained from the Information Commissioner.

15.4 Right to Prevent Processing for Direct Marketing.

The trust will not process Personal Data for direct marketing purposes although we may contact members informing them of products or services.

15.5 Right to Rectification, Blocking, Erasure and Destruction.

Although the exercising of this right is normally achieved by a court order, the trust will rectify, block, erase or destroy data relating to a member, which has been shown to be incomplete, inaccurate or stored in a manner incompatible with the legitimate purposes of the data controllers. The onus is on the data subject to advise the trust, in writing, which data is incomplete or inaccurate. The DPO will ensure that the rights of the data subject are met as far as practicable and will respond in writing on behalf of the data controllers. If the data subject remains concerned or unhappy with the course of action taken, he or she can seek remedy through the courts.

16.0 **Enforcement**

16.1 Any person who believes that (s)he is being directly affected by the processing of personal data may apply to the Information Commissioner for an assessment on whether the processing is being carried out in compliance with the DPA 98. This may require the Commissioner to initiate a formal criminal investigation or a civil investigation. In the case of the latter, the Commissioners compliance department will consider whether the alleged breach requires the issue of an Enforcement Notice or some other action is merited. If it is likely that an Enforcement Notice will be issued, the Compliance Department will seek the written views of the Data Controllers. The DPO is to provide the data controllers with a draft response to enable them to reply within 28 days.

16.2 Information Notice

The Commissioner may serve an Information Notice on the data controllers, requiring them to furnish specific information. The notice will include a time limit imposed by the Commissioner. The DPO is to provide the data controllers with a draft response to enable them to respond within the stipulated time limit.

16.3 Enforcement Notice

When the Commissioner is satisfied that the data controllers have contravened or are contravening the Data Protection principles, he may serve an Enforcement Notice requiring the data controllers to take specific rectification action. The notice will include a time limit, which commences the day that the notice is served. The DPO is to ensure that either:

- the terms of the Enforcement Notice are complied with, or
- an appeal against the terms (if justified) is lodged in accordance with the DPA 98

APPENDIX A

Procedure for Subject Access Requests

Background

The BWFCST processes personal data in respect of members and third parties; these are the data subjects. Data subjects are entitled to be told whether the trust, or someone else on its behalf, is processing their Personal Data. Providing that the data subject submits his/her request in accordance with these procedures, the Data Subject is entitled to receive:

- a description of the personal data of which the individual is the data subject
- a description of the purposes for which the data is being processed
- a description of the recipients to whom the data are or may be disclosed
- a copy, in a form that is capable of being understood, of:
  - the information constituting any personal data of which he is the data subject
  - any information as to the source of that data

The Subject Access request procedure will ensure that personal data are made available to the data subject in a timely manner.

Prerequisites

The Data Subject must submit the request in a written permanent form including e-mail. The written request must contain sufficient information to reasonably satisfy the Data Controllers as to the identity of the applicant and to locate the information that the person seeks. The written subject access request is to be accompanied with a cheque for £10 made payable to "BWFCST", which is the statutory fee applicable in the UK for processing the request. The Data Controllers may waive the charge and, if they do, the cheque will be returned.

Subject Access Request Procedure

All requests from data subjects for access to their personal data processed by the trust must be passed to the DPO who will coordinate data collection and respond to the request.

- the Trust is constrained by law to respond within 40 Calendar days commencing the day that the request is received

The DPO is to ensure that any response is communicated to the data subject in a form that is capable of being understood.

Where there is a danger that the DPO may not be able to respond within 40 days, the board are to be advised immediately and wherever possible no later than the 20th day of processing the request.

A record of each request is to be maintained using a suitable recording format. The DPO is to ensure that the record is stored and available for inspection.

No attempt is to be made by the Trust to subvert, destroy or deny personal data which is the subject of an access request.

If, in the course of normal business, it is necessary to amend personal data (by addition or deletion) whilst a subject access request is being processed, it is permissible to provide the data subject with the amended data but only where the amendment would have been made regardless of the subject access request. In other words, data cannot be altered after a request has been received in order to obfuscate the objectives of the request.

The Trust recognizes that it does not have to comply with a subject access request where the disclosure of such information is likely to result in another data subject being identified. In such cases the Trust will refuse access unless:

- the third party has consented to the disclosure of the information to the person making the request, or
- it is reasonable and lawful to comply with the request without the consent of the third party

Where the DPO considers that provision of the data would result in effort that was disproportionate to the benefit to be derived by the data subject, the board is to be notified immediately so that an assessment can be made. The onus is on the Data Controllers to be able to show that the effort was disproportionate.