AFC Wimbledon Foundation

The Cherry Red Records Stadium
Jack Goodchild Way
422A Kingston Road
Kingston upon Thames
Surrey
KT1 3PB

Data Protection Policy

Authorised Signatory	Title	Date
Philip Rudling	Data Protection Officer	10/05/18
Erik Samuelson	Chair of Trustees	10/05/18

Signature Philip Rudling

Signature Erik Samuelson

Definitions: In this policy, the following words and phrases have the following meaning:

Accessible Record	Any data to which there is a statutory right of access
Act	The Data Protection Acts 1998 and 2018 plus the EU General Data Protection Regulations and any other UK legislation in force from time to time.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes signifying their agreement to the processing of personal data relating to them
Personal Data	Information which relates to an individual who is ● Living ● Identifiable directly or indirectly (from that data or from other data held by the Data Controller) Personal Information includes ● name ● address ● date of birth ● email address ● telephone number(s) ● relationship to other data subjects and which: ● is processed by means of equipment operating automatically in response to instructions given for that purpose or ● is recorded with the intention that it should be so processed or ● is recorded as part of a relevant structured filing system or with the intention that it should form part of such a system or ● does not fall within the above but forms part of an accessible record Automated data ● computer records / systems ● emails ● audio/video ● CCTV and digitised images ● Document image processing Manual data ● Paper files
Member of staff	Is any director, employee, worker, agency worker, intern, work experience, contractor, and consultant employed or engaged by the Foundation
Data Controller	The person(s) (Foundation Director) who determines what personal information the Foundation will hold,

	how it will be held and the manner in which this is to be processed
Data Processor	Any person who processes the data on behalf of the Data Controller
Data Protection Officer (DPO)	The employee appointed by the Board to be responsible for all matters relating to the Foundation's compliance with the Act
Data Subject	An living individual who is the subject of personal data held by the Foundation
Processing	Obtaining, recording, amending, organising, handling, storing, erasing, destroying or disclosing personal or sets of personal information whether or not by automated means. It also includes transmitting or transferring to a third party
Recipient	Any person to whom data is disclosed including any person to whom it is disclosed in the course of processing (e.g. an employee or agent of the data controller)
Structured filing system	Any set of information relating to individuals where – although the information is not automatically processed – the set is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible
Sensitive personal data	Personal data relating to ● racial or ethnic origin ● political opinions ● religious beliefs or beliefs of a similar nature ● membership of a Trade Union ● physical or mental health or condition ● sexual life ● criminal convictions and offences and data relating to criminal allegations and proceedings
Third party	Any person other than ● the data subject ● the data controller ● the data processor or other persons authorised to process data for the data controller or processor

1. Introduction

AFC Wimbledon Foundation is committed to a policy of protecting the rights and privacy of individuals. We need to collect, use and retain certain types of personal data in order to carry out our work. This information must be collected and handled securely. Protecting the confidentiality, security and integrity of the personal data that the Foundation processes is of paramount importance to its business operations.

The Act set out the lawful use of information about people (personal data). Personal information can be held on desk top computers, lap tops manual devices or in manual paper files and includes emails and photographs including CCTV footage.

The legislation is designed to protect individuals from:

- the use of incorrect information about them, whether that information is automatically processed (e.g. computer records or CCTV footage) or held in non-automated structured filing systems (i.e. paper based records)
- the improper use of correct information held to ensure the Foundation's compliance with the legislation on the protection of individuals with regard to the processing of personal data.

The Board of Trustee's is the "Data Controller" for the information held. Members of staff are personally responsible for protecting and using personal information in accordance with the DPA and GDPR. All members of staff will therefore be required to read, understand and comply with this policy.

The aim and purpose of the policy is to ensure the club's compliance with the Data Protection Acts. It applies to all members of staff.

Members of staff are also data subjects.

The club's Data Protection Officer (DPO) has responsibility for data protection compliance and should be contacted if there any questions about the operation of this policy or if further information is required about data protection. Additionally if a member of staff believes that this policy has not been followed or there has been a data breach they should contact the DPO or they can raise a formal grievance under the club's grievance procedure.

2. Purpose

The purpose of this policy is to set out the club's commitment for protecting personal data. **More details of the policy framework are shown at Appendix 1**. The Board of Trustees regard the lawful and correct processing of personal information as a priority as it maintains the confidence of those that the Foundation deal with on a day to day basis. They recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The Board recognises the Foundation must be able to demonstrate compliance with the data protection principles set out below. This means that the club must implement appropriate and effective technical and organisational measures to ensure compliance.

3. The Data Protection Principles

The Foundation will comply with the 6 principles contained in the Act. The Foundation and all members of staff must comply with these at all times in their data processing activities taking steps to ensure that personal information is:

1. **fairly and lawfully processed in a transparent manner** (and will not be processed unless specific conditions are met). Processed in accordance with the data subject's rights under the legislation;

2. **obtained and processed for explicit specified and legitimate purposes** and not further processed in any manner incompatible with those purposes;

3. **adequate, relevant and not excessive** to the required purpose;

4. **accurate and where necessary kept up-to-date;**

5. **not kept for longer than necessary;** and

6. **kept secure by the "Data Controller"** who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to personal information.

More specific details on these principals are set out in Appendix 2

4. Access by Data Subjects

The Foundation will ensure compliance with the rights of data subjects to:

- have a copy of information held;
- have it corrected if it is inaccurate, lost or disclosed in inappropriate circumstances;
- complain if they suffer damage or distress because of information being inaccurate, lost or disclosed in inappropriate circumstances;
- prevent processing likely to cause damage or distress;
- request to erasure of data i.e. "right to be forgotten";
- prevent processing for the purposes of direct marketing;
- be informed by the Data Controller of the logic involved in any automatic decision making (i.e. the processing of personal data by automatic means for the purpose of evaluating matters relating to the individual where such processing has formed the sole basis for any decision significantly affecting that person); and
- request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

The Foundation will respond positively and promptly to Subject Access Requests (SAR), following the agreed SAR process (Appendix 1 and 4). There is also a separate procedure note on the SAR process.

Whilst individuals have a general right of access to any of their own personal information which is held, the Foundation will be mindful of those circumstances where an exemption may apply and, in particular, the data protection rights of third parties who may also be identifiable from the data being requested.

The Foundation will always seek the permission of the data subject, where it is required by law to do so.

5. Members of Staff

The Foundation will ensure that all members of staff are advised of their rights as data subjects under the Act.

The Foundation will ensure that all members of staff with responsibility for the processing of personal data are appropriately trained and aware of their data protection obligations and liabilities under the Act. **(Appendix 3 for guidelines)**

Foundation managers are responsible for:

- ensuring that the data protection requirements are carried out;
- providing clear messages to their staff regarding appropriate processing of the personal data that they handle;
- in conjunction with the Foundation's DPO identifying and addressing training needs within their teams;
- consulting the DPO before processing data for a new purpose
- advising the DPO of any SARs or complaints

All members of staff are responsible for:

- complying with the data protection principles as supported by this policy, guidance on the application of this policy and associated policies such as the Foundation's ICT policy and Code of Conduct;
- contacting their manager or DPO for guidance or if they are in any doubt about how they should deal with any piece of personal data; and
- only processing personal data in the manner it was authorised for the purpose of carrying out their responsibilities or with management authorisation

All members of staff must ensure they are aware that a breach of the procedures indentified in this policy may lead to disciplinary action taken against them.

All members of staff will be made aware that all materials held on Foundation equipment (including desk top computers, laptops, mobile phones and electronic organisers) may be subject to:

- monitoring; and
- search for example, in the course of processing SARs.

This includes any personal materials (letters, emails etc) being held on Foundation equipment by a member of staff.

The Foundation takes compliance with this policy very seriously. Any breach of this policy or Data Protection legislation will be regarded as misconduct under the Foundation's Code of Conduct and dealt with according to the rules set out.

If the non compliance is by any other person than a Director or employee the contract or work arrangement will be terminated with immediate effect.

6. Third Party Suppliers

Where the Foundation uses third-party service providers to process personal data on their behalf, additional security arrangements need to be implemented in contracts with those third parties to safeguard the security of personal data. Certain safeguards and contractual arrangements should be put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services;
- sharing the personal data complies with the privacy notice that has been provided to the data subject (and, if required, the data subject's consent has been obtained);
- the third party has agreed to comply with the Foundation's data security procedures and has put adequate measures in place in ensure the security of processing;
- the third party only acts on the Foundation's documented written instructions:
- a written contract is in place between the Foundation and the third party that contains specific approved terms;
- the third party will assist the Foundation in allowing data subjects to exercise their rights in relation to data protection and in meeting the Foundation's obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the third party will delete or return all personal data to the Foundation at the end of the contract; and
- The third party will submit to audits.

7. Security

6.1 General

The Foundation will ensure that

- appropriate security measures are in place to protect personal data, both automated and manual systems on either internal or third party systems;
- personal data systems are accessible to authorised members of staff; and
- authorised members of staff using these systems will be advised of appropriate security procedures and the importance of their role within these procedures.

6.2 Use of Email

The Foundation's email system is used for the transmission of sensitive personal data (e.g. staff, participant personal data, HR matters). Members of staff are required to note that the route by which e-mail is delivered is often circuitous and may even involve being exposed to very insecure networks. Marking such emails "Private and Confidential" does not ensure their security. Foundation email accounts should only be used on official business

6.3 Risk Management

The accidental or deliberate disclosure of "sensitive" information or the retention of information for longer than required have been identified as potential risks in the Foundation's Data Protection Risk Register.

8. Resources

The Foundation will allocate such resources as may be required to ensure the effective operation of this policy.

9. Responsibility

The DPO will have overall responsibility for the administration and implementation of the club's Data Protection Policy. Each Manager will assume responsibility for the compliance of staff within their department.

The Foundation's DPO will provide advice and guidance on implementation of the Act.

10. Linkages to other Foundation Policies

A number of other policies of the Foundation should be read in conjunction with this policy, including:-

10.1 Information & Communications Technology Policy

The Foundation's ICT policy includes the following:

- security policy;
- protection of hardware from theft and accidental loss;
- protection of data from unauthorised access;
- reporting of IT security breaches;
- use of portable devices (laptop computers, etc); and
- personal use by staff of Foundation owned systems and equipment

Any breach of the ICT policy may result in:

- denial of ICT equipment/services for a period or permanently
- disciplinary action through the Foundation's disciplinary process
- provision of information to the police for possible criminal proceedings.

10.2 Code of Conduct for Foundation Employees

The "Code of Conduct for Foundation Employees" includes reference to the disclosure of information and notes that personal information held about individuals must be treated in accordance with the legislation. Any breach of the terms of this code will be dealt with in accordance with the provisions of the Foundation's Disciplinary Procedure.

10.3 Data Retention Policy

The Data Retention Policy includes reference to periods where personal identifiable data is held and where it is archived.

10.4 Subject Access Request Policy and Procedure

This policy sets out the step by step process to follow when the Foundation receives a Subject Access Request

11. Review

This policy will be reviewed regularly and relevant personnel advised of any amendments/updates.

The policy will also be reviewed in the event of

:

- changes in legislative requirements
- changes in Foundatio policy
- weaknesses in the policy being highlighted

The Foundation will introduce regular reviews of privacy measures, policies, procedures and contracts. The DPO will regularly test the club's systems and processes to monitor and assess ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

Appendix 1

FRAMWORK FOR DATA PROTECTION PROCEDURES

1. Applying the Data Protection Act within the Foundation

The Foundation will let people know why we are collecting data, and for what purpose It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to authorised members of staff.

2. Data access, correction and erasure

Individuals have the right to make a Subject Access Request (SAR) to find out whether the Foundation holds their personal data, where it is, what it is used for and to have the data corrected or erased, to prevent use which is causing them damage or distress or to stop marketing information being sent to them. Any SAR will be replied to within 21 calendar days by the Foundation's DPO. Steps will be taken to confirm the identity of the individual before providing the information.

The SAR application form is set out at Appendix 3

3. Responsibilities

The Foundation Board of Trustees

The Board of Trustees is the Data Controller under the legislation and is legally responsible for determining what purpose personal information held will be used for. They will take into account all legal requirements when determining appropriate management control. They will ensure strict application of the following criteria regarding personal information:

- collected and use information lawfully and carefully;
- specify the purpose for which information is used;
- use and process information only to the extent that it is needed to fulfil the operational need or to comply with any legal requirement;
- ensure the quality of the information used;
- ensure the rights of individuals about whom the identity held can be exercised under the act
    - The right to be informed that processing is undertaken
    - The right of access to one's personal information
    - The right to prevent processing
    - The right to be forgotten
    - The right to correct, rectify, bloc or erase information that is regarded as incorrect;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure personal information is not transferred abroad without suitable safeguards;
- treat people fairly and justly whatever their age, religion, disability, sexual orientation or ethnicity when dealing with requests for information; and
- set out clear procedures for dealing with Subject Access Requests (SAR)

Members of staff

All staff must ensure they are aware that a breach of the procedures indentified in this policy or Data Protection legislation will lead to disciplinary action taken against them under the Foundation's Code of Conduct.

Data Protection Officer (DPO)

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- ensuring every member of staff processing personal information understands that they are responsible for following good data protection practices;
- ensuring every member of staff processing personal information is appropriately trained to do so;
- ensuring every member of staff processing personal information where necessary is appropriately supervised;
- ensuring every member of staff can describe how the Foundation handles personal information;
- ensuring every member of staff wanting to make enquiries about handling personal information knows what to do;
- ensuring the Foundation complies with its SAR policy and procedures;
- dealing promptly and courteously with any enquiries about handling personal information;
- regularly reviewing and auditing the way the Foundation holds, manages and uses personal information; and
- regularly assessing and evaluating the Foundation's performance in relation to handling personal information

The DPO can be contacted at Philip.rudling@afcwimbledonfoundation.org.uk

4. Personal Information held by Staff on Foundation / Club Owned Equipment

All materials held on Foundation / Club equipment (including desk top computers, laptops, mobile phones and electronic organisers) may be subject to:

- monitoring; and

- search, for example, in the course of processing Data Protection SARs

This includes any personal materials (letters, emails etc) being held on Foundation /club equipment by a staff member.

5. Foundation / Club's policy on the Use of Equipment and Assets

This policy prohibits the extensive use of Foundation / Club equipment by members of staffs for any use unrelated to their employment or letter of understanding agreement with AFC Wimbledon Foundation or AFC Wimbledon Ltd.

6. Foundation's email policy

The content of e-mail is subject to all applicable UK laws such as those relating to copyright, defamation, data protection and public records.

If a member of staff keeps copies of e-mail or other communications for any length of time, they must be aware that they are almost certain to be "personal data" within the terms of the Data Protection legislation, e.g. email address.

The Foundation reserves the right to monitor, where appropriate, e-mail usage. This will mean monitoring e-mail content and providing such details and statistics to appropriate managers. Where violation of this email policy occurs an investigation will be carried out which may lead to disciplinary action being taken.

7. Notification

The Foundation will ensure that the regulatory authorities are advised of all notifiable uses of information, as required under the legislation. The Foundation will conduct periodic reviews and update these register entries whenever necessary.

Appendix 2

DETAILS OF DATA PROTECTION PRINCIPLES

1. Fairly and Lawfully Processed in a Transparent Manner

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle means that both the Foundation and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

The data protection legislation (article 6 of EU regulations) provides that processing is only lawful in cetain circumstances. These include where:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;

- the processing is necessary for the performance of a contract with the data subject e.g. an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract;

- the processing is necessary for compliance with the Foundation's legal obligations:

- the processing is necessary to protect the data subject's vital interests (or someone else's vital interests);

- the processing is necessary to pursue the Foundation's legitimate interests or those of a third party, where the data subject's interests or fundamental rights and freedoms do not override the Foundation's interests; the purposes for which the Foundation process personal data for legitimate interests must also be set out in an appropriate privacy notice.

When the Foundation relies on consent as the lawful basis this requires the data subject to have given a positive statement, active opt in or a clear action. Member of staff must contact the DPO for advice if the plan is to use prior consents for a new data processing activity.

The data protection legislation (article 9 of EU regulations) also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies. All staff must check with the DPO if they intend to process the following information:

- health and medical records
- racial or ethnic origin
- political affiliation
- sexual orientation
- religious or similar beliefs
- trade union membership
- criminal records

The Foundation must keep a record of all consents, including explicit consents, which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables the Foundation to demonstrate compliance with the data protection requirements for consent.

Under the data protection legislation (article 13 of EU regulations), the transparency principle requires the Foundation to provide specific information to data subjects through privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices will state general privacy statements applicable to groups of data subjects.

The Foundation's general privacy statement is located on the shared drive in the "Data Protection-Polices" folder or a copy can be obtained from the Foundation DPO

2. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes (article 5(1.b) of EU regulations)

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, unless the data subject has been informed of the new purposes and the terms of this policy are otherwise complied with e.g. there is a lawful basis for processing. This also includes special categories of personal data and criminal records personal data.

Member of staff must contact the DPO for advice if they plan is to use previously obtained personal data for a new data processing activity.

3. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (article 5(1.c) of EU regulations)

The club will only collect personal data to the extent that it is required for the specific purposes notified to the data subject. Members of staff must ensure that any personal data collected is adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

4. Accurate and where necessary kept up-to-date

Personal date must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. (article 5(1.d) of EU regulations)

The Foundation must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. It must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

5. Not kept for longer than necessary

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (article 5(1.e) of EU regulations).

The Foundation only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which it was originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special categories of personal data and criminal records personal data.

Please refer to the Foundation's data retention policy for more details.

6. Kept secure by the "Data Controller"

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (article 5(1.f) of EU regulations)

The Foundation takes the security of personal data seriously and has implemented and maintained safeguards which are appropriate to the size and scope of the Foundation, the amount of personal data that the Foundation hold and any identified risks.The Foundation has also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of the it's processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored tn a timely manner. The Foundation regularly test and evaluate the effectiveness of its technical and organisational safeguards to ensure the security of the Foundation's processing activities.

Please refer to the Foundation's ICT policy for more details.

Accountability

.
The Foundation must be able to demonstrate compliance with the data protection principles set out above. (article 5.2 of EU regulations)This means that the Foundation must implement appropriate and effective technical and organisational measures to ensure compliance To this end the club has / will:

- appointed a Data Protection Officer to be responsible for data protection compliance and privacy matters within the Foundation;

- keep written records of personal data processing activities;

- implement a privacy by design approach when processing personal data and the Foundation will conduct and complete data protection impact assessments (DPIAs) where a type of data processing,, process or IT system, in particular using a new technology, is likely to result in a high risk to the rights of data subjects;

- integrate data protection requirements into the Foundation's internal documents, including this data protection policy, other related policies and privacy notices; and

- introduce a regular training programme for all members of staff on the data protection legislation and on their data protection duties and responsibilities and the Foundation also maintain a training record to monitor its delivery and completion

Appendix 3

GUIDELINES FOR MEMBERS OF STAFF ON DATA PROTECTION

Some members of staff will process data about participants and customers of the Foundation (e.g. school children, parents, sponsors, adult clients). The Foundation will ensure through
procedures, that all participants and customers give their consent to processing and retention of personal data as required by the Data protection legislation.

The information that staff process on a day-to-day basis will be standard and will cover categories such as:

- name
- postal address
- email address
- date of birth
- bank details
- contact telephone numbers

All members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the club's Data Protection Policy.

In particular members of staff must ensure that records are:

- fairly and lawfully processed
- obtained and processed lawfully
- adequate, relevant and not excessive
- accurate and kept up-to-date
- not kept for longer than necessary
- processed in accordance with the data subject's rights under the legislation
- kept secure

The Foundation will designate staff who will be the only staff authorised to hold or process data that is personally sensitive. This includes:

- health and medical records
- racial or ethnic origin
- political affiliation
- sexual orientation
- religious or similar beliefs
- trade union membership
- criminal records

Staff shall not disclose personal data to any other member of staff except with the authorisation or agreement of the line manager or DPO, or in line with Foundation policy.

Members of staff must only process personal data where their job duties and responsibilities require it and they must not process personal data for any reason which is unrelated to their job duties and responsibilities.

Before processing any personal data, all members of staff should consider the checklist below:

- have you reviewed the purpose of processing the information selecting the lawful basis of processing?
- have you been given the consent by the data subject to process their information?
- do you really need to record the information?
- is the information ‘standard’ or is it ‘sensitive’?
- if it is sensitive, do you have the authority to do so and the data subject’s express consent?
- has the customer been told that this type of data will be processed?
- are you authorised to collect/store/process the data?
- if yes, have you checked with the data subject that the data is accurate?
- are you sure that the data is secure?
- if you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the club to collect and retain the data?

Member of staff should contact the DPO to seek further advice in the following circumstances:

- if you are in any doubt about what you can or cannot disclose and to whom;
- if you are unsure about the lawful basis you are relying on to process personal data
- if you need to rely on consent to process personal data
- if you are not clear about the retention period for the personal data being processed
- if you are unsure about what appropriate security measures you need to implement to protect personal data If you need assistance in dealing with any rights invoked by a data subject
- if you suspect there has been a personal data breach
- where you propose to use personal data for purposes other than that for which they were collected
- where you intend to engage in a significant new or amended data processing activity

- where you plan to undertake any activities involving automated decision-making, including profiling

- if you need assistance with, or approval of, contracts in relation to sharing personal data with third-party service providers

- if you believe personal data are not being kept or deleted securely or are being accessed without the proper authorisation

- if you suspect there has been any other breach of this policy or any breach of the data protection principles

In Summary

- only access personal data that you have authority to access and only for authorised purposes e.g. if you need it for the work you do for the Foundation, and then only use the data for the specified lawful purpose for which they were obtained;

- only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally;

- do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Foundation's website or posted on the iternet in any form, unless the data subject has given their explicit consent to this;

- be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request;

- where the Foundation provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Foundation's requirements in this regard;

- only transmit personal data between locations by e-mail if a secure network is in place e.g. encryption is used for e-mail;

- if you receive a request for personal data about another member of staff or data subject, you should forward this to the Foundation's DPO; and

- ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with the Foundation's policy on computer access and secure file storage.

Please note:

It is important that the personal data the Foundation hold about you as a data subject is accurate and up to date. Please keep the Foundation informed if your personal data changes so that club's records can be updated. The Foundation cannot be held responsible for any errors in your personal data in this regard unless you have notified the Foundation of the relevant change. The Foundation will promptly update your personal data if you advise that the information has changed or is inaccurate.

Appendix 4

Personal Data Access Request Form

General Data Protection Regulations from 25 May 2018

This legislation gives participants, customers, parents of schoolchildren, adult clients and staff of AFC Wimbledon Foundation the right to know what personal information about them is held by the Foundation in either electronic or paper format. You can apply to the Foundation to release this information to you by completing this request form. Requests relating to information held by AFC Wimbledon Foundation should be directed to Data Protection Manager, Philip Rudling.

The Foundation needs proof of the identity of the person concerned (the 'Data Subject') before relevant data is released. Please note that the Foundation will endeavour to respond within 21 days but may need a maximum of 60 days in which to supply the requested information, and that the Foundation reserves the right to obscure or suppress information that relates to third parties.

1 Are You the Data Subject?

Yes – You will need to supply the Foundation with evidence of your identity (e.g. passport, photographic ID card, or proof of address such as a utility bill) as well as the completed form. This is to ensure that we release data only to those who have a legal right to see the information.

No – Are you acting on behalf of the Data Subject with their authority? If so, you will need to enclose the original copy of their written authorisation along with this form (which can be a letter signed personally by the Data Subject) so that the Foundation can confirm that this request relates to the Data Subject. You will be the Applicant and therefore you will be required to supply the evidence of your identity as if you were the Data Subject. You should enter the details of the Data Subject in Section 3 below.

Now complete sections 2, 3 (if applicable), 4 and 5.

2 Details of Applicant

Name……

Full address (including postcode)……..

…….

Telephone number……

Email address……...

3 Details of the Data Subject (if different to 2)

Name……

Full address (including postcode)……..

…….

Telephone number……

Email address……...

Why are you making this request on behalf of the Data Subject?

……

……

4 Foundation contact: please provide details of your data relationship with the club, e.g. staff member, current or previous holiday course participant / parent, schoolchild participant in schools coaching programmes, participant on afterschool / early evening sessions, adult participant, eg walking football

……

……

5 Information Required

If you wish to know whether the Foundation holds a specific piece of information on the Data Subject, please state it here. If this section is left blank, all the information the club holds on the Data Subject will be provided.

……

……

Signed……

Date…….

You can return this form in either of two ways:

by post, including a photocopy of proof of ID, to The Data Protection Officer, AFC Wimbledon Foundation, The Cherry Red Records Stadium, Jack Goodchild Way, Kingston upon Thames, KT1 3PB

by email, along with a scan of proof of ID, to
Philip.rudling@afcwimbledonfoundation.org.uk