FORMBY VILLAGE SPORTS CLUB

DATA PROTECTION POLICY

Formby Village Sports Club (**FVSC**) is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all members, directors and volunteers. (**Members**).

This Data Protection Policy (**Policy**) sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data. ***Please pay special attention to sections 13, 14 and 15 as these set out the practical day to day actions that you must adhere to when working or volunteering for the club.***

This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact *the club's Data Protection Officer.*

Who is responsible for data protection?

1.1 All our members are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2 We have appointed Christine Hosie to be responsible for overseeing our compliance with data protection laws and she has the title of Data Protection Officer.

1.3 **Why do we have a data protection policy?**

1.4 We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our Club. We believe that such relationships will enable our Club to work more effectively with and to provide a better service to those individuals.

1.5 This Policy works in conjunction with other policies implemented by us from time to time.

2. **Status of this Policy and the implications of breach.**

2.1 Any breaches of this Policy will be viewed very seriously. All members must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.

2.2 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the Data Protection Officer. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date this Policy coming into force.

2.3 Also, if you are aware of or believe that any other representative of ours is not complying with Data Protection Laws and/or this Policy you should report it in confidence to the Data Protection Officer.

3. **Other consequences**

3.1 There are a number of serious consequences for both yourself and the Club if we do not comply with Data Protection Laws. These include:

3.1.1 For you:

3.1.1.1 **Disciplinary action:** As a member your terms and conditions of membership require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. If you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

3.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

3.1.1.3 **Investigations and interviews**: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

3.1.2 For the Club:

3.1.2.1 **Criminal sanctions:** Non-compliance could involve a criminal offence.

3.1.2.2 **Civil Fines:** These can be up to € 20 million or 4% of turnover whichever is higher.

3.1.2.3 **Assessments, investigations and enforcement action**: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner.

3.1.2.4 **Court orders:** These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

3.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of our non-compliance.

3.1.2.6 **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to the Information Commissioner quickly become public knowledge and might damage our Club.

3.1.2.7 **Loss of business:** Prospective members, participants, players, customers, suppliers and contractors might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.

3.1.2.8 **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes time and effort and can involve considerable cost.

4. **Data protection laws**

4.1 The General Data Protection Regulations (**GDPR**) require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data.

5. **Key words in relation to data protection**

5.1 **Personal data** is data that relates to a living individual who can be identified from that data. That personal data might be written, oral or visual (e.g. CCTV).

5.2 **Identifiable** means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable).

5.3 **Processing** - generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

5.4 **Data controller** is the person who decides how personal data is used. FHTSC will always be a data controller in respect of personal data relating to our members.

5.5 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller.

6. **Personal data**

6.1 Data will relate to an individual and therefore be their personal data if it:

6.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

6.1.2 affects the individual's privacy, whether in their personal, family, organisation or professional capacity.

7. **Lawful basis for processing**

7.1 For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

7.2 For the processing of ordinary personal data in our club these may include, among other things:

7.2.1 the data subject has given their consent to the processing

7.2.2 the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);

7.2.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject (such as reporting employee PAYE deductions to the tax authorities); or

7.2.4 the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members, players, participants about competition dates, upcoming fixtures or access to club facilities).

8. **Special category data**

8.1 Special category data under the Data Protection Laws is personal data relating to an individual's race, health, religious or other beliefs etc. Criminal records history becomes its own special category which is treated for some parts the same as special category data.

8.2 To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

8.2.1 the processing is necessary for the performance of our obligations under employment law;

8.2.2 the processing is necessary to protect the vital interests of the data subject.

8.2.3 the processing relates to information manifestly made public by the data subject;

8.2.4 the processing is necessary for the purpose of establishing, exercising or defending legal claims.

8.3 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

8.3.1 ensure that either the individual has given their explicit consent to the processing; or

8.3.2 ensure that our processing of criminal records history is necessary under a legal requirement imposed upon us.

8.4 We would normally only expect to process special category personal data or criminal records history data in the context of our members/coaches/volunteers for safeguarding checks etc.

8.5 **When do we process personal data?**

8.6 Virtually anything we do with personal data is processing. We might process personal data using computers or manually by keeping paper records.

9. **Outline**

9.1 In summary, data protection law requires each data controller to:

9.1.1 only process personal data for certain purposes;

9.1.2 process personal data in accordance with the 6 principles of 'good information handling'

9.1.3 provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice,

9.1.4 respect the rights of those individuals about whom we process personal data and

9.1.5 keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

9.2 Every member has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

9.3 Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

10. Data protection principles

10.1 The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

10.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

10.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

10.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

10.1.4 accurate and where necessary kept up to date;

10.1.5 kept for no longer than is necessary for the purpose ("storage limitation");

10.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

11. Data subject rights

11.1 Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

11.1.1 The rights to access their personal data, usually referred to as a subject access request

11.1.2 The right to have their personal data rectified;

11.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

11.1.4 The right to restrict processing of their personal data;

11.1.5 The right to object to receiving direct marketing materials;

11.1.6 The right to portability of their personal data;

11.1.7 The right to object to processing of their personal data.

11.2 The exercise of these rights may be made in writing, including email, and also verbally and should be responded to in writing by us without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

11.3 Where the data subject makes the request by electronic means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

11.4 If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request.

11.5 There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right to not receive marketing material is an absolute right, so this should be complied with immediately.

11.6 Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation.

11.7 In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation.

11.8 In the event of a member receiving such a notice, they must immediately pass the communication to our Data Protection Officer.

12. Notification and response procedure

12.1 If a member has a request or believes they have a request for the exercise of a Right, they should:

12.1.1 try to get the request confirmed in writing addressed to our Data Protection Officer and

12.1.2 inform our Data Protection Officer of the request.

12.2 If a letter or email exercising a Right is received by any member they should:

12.2.1 pass the letter to the Data Protection Officer;

12.2.2 our Data Protection Officer will then respond to the data subject on our behalf.

12.3 Our Data Protection Officer will co-ordinate our response. The action taken will depend upon the nature of the request. The Data Protection Officer will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the Data Protection Officer should suffice in most cases.

12.4 The Data Protection Officer will inform the relevant management line of any action that must be taken to legally comply. The Data Protection Officer will co-ordinate any additional activity required to meet the request.

12.5 The Data Protection Officer's reply will be validated by the relevant Section Head producing the response. For more complex cases, the letter/email to be sent will be checked by legal advisors.

13. Your main obligations

13.1 What this all means for you can be summarised as follows:

13.1.1 Treat all personal data with respect;

13.1.2 Immediately notify your Section Head or the Data Protection Officer if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

13.1.3 Take care with all personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

13.1.4 Immediately notify the Data Protection Officer if you become aware of or suspect the loss of any personal data or any item containing personal data.

14. **Your activities**

14.1 You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

15. **Practical matters**

15.1 Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

15.1.1 Never leave any items containing personal data unattended in a public place or unsecure location and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

15.1.2 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

15.1.3 Do password protect documents and databases containing personal data.

15.1.4 Never use removable storage media to store personal data unless the personal data on the media is encrypted.

15.1.5 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

15.1.6 Do challenge unexpected visitors accessing personal data.

15.1.7 Do not leave personal data lying around, store it securely.

15.1.8 When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

15.1.9 Do not transfer personal data to any third party without prior written consent of your Section Head or our Data Protection Officer.

15.1.10 Do notify your Section Head or our Data Protection Officer immediately of any suspected security breaches or loss of personal data.

15.1.11 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our Data Protection Officer.

16. **Foreign transfers of personal data**

16.1 Personal data must not be transferred outside the European Economic Area (**EEA**).

17. **Queries**

17.1 If you have any queries about this Policy please contact the Data Protection Officer.