2.4 DATA PROTECTION POLICY

1 Policy

1.1 Yeovil & Sherborne Hockey Club (the **Club**) is committed to complying with data protection law and to respecting the privacy rights of individuals.

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

1.3 This **Policy** applies to all club members including its officers and volunteers, as well as any employees and contractors (the **Members**).

1.4 The **Club** recognises that processing of individual member's personal information in a careful and respectful manner cultivates trusting relationships with those members and trust in the **Club**'s reputation. The **Club** believes that such relationships will enable the **Club**'s organisation to work more effectively with and to provide a better service to those members.

1.5 This **Policy** works in conjunction with other policies implemented by the **Club** from time-to-time.

1.6 All **Members** have a role to play in achieving these aims. It is their responsibility, therefore, to familiarise themselves with this **Policy** and to apply and implement its requirements when processing any personal information.

1.6.1 Special attention should be paid to Sections 13, 14 and 15 as these set out the practical day-to-day actions that **Members** must adhere to when working or volunteering for the club.

1.7 Data protection law is a complex area. This **Policy** has been designed to ensure that **Members** are aware of the legal requirements imposed on them and on the **Club**, and to give **Members** 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 the **Club**'s or its **Members'** responsibilities in relation to data protection.

1.8 If at any time **Members** have any queries on this **Policy**, their responsibilities or any aspect of data protection law, they should seek advice from the Club Chairman, Club Secretary, Membership Secretary or Welfare Officer (see Section 3) Full contact details are on the contacts page of the **Club**'s website.

2 Definitions

2.1 The following definitions are used in this **Policy**:

2.1.1 **"Personal Data"** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into the **Club**'s possession). That living individual might be a member, volunteer, employee, contractor, prospective member, supplier, or contact, and that personal data might be written, oral or visual.

2.1.2 **"Identifiable"** means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable the **Club** (e.g. a job title and company name).

2.1.3 **"Data Subject"** is the living individual to whom the relevant personal data relates.

2.1.4 **"Processing"** is widely defined under data protection law and generally any action taken by the **Club** 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 images.

2.1.5 **"Data Controller"** is the individual or organisation who decides how personal data is used, for example the **Club** will always be a data controller in respect of personal data relating to the **Club**'s members.

2.1.6 **"Data Processor"** is an individual or organisation who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example FullOnSport will be a data processor.

3 Responsibility

3.1 All of the **Club**'s officers, volunteers, employees and contractors are responsible for data protection, and each **Member** has their role to play to make sure that the **Club** is compliant with data protection laws.

3.2 The **Club** is not required to appoint a Data Protection Officer (DPO). However, because of their roles, four **Club** officers (Club Chairman, Club Secretary, Membership Secretary and Welfare Officer – the **Data Protection Working Group**) have responsibility for overseeing the Club's compliance with data protection laws. Full contact details are on the contacts page of the **Club**'s website.

4 Laws

4.1 The Data Protection Act 1998 (DPA) applies to any personal data that the **Club** process, and from 25 May 2018 this will be replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (together "Data Protection Laws") and then after Brexit the UK will adopt laws equivalent to these Data Protection Laws.

4.2 This **Policy** is written as though GDPR and the DPA 2018 are both in force, i.e. it states the position as from 25th May 2018.

4.3 Data Protection Laws all require that the personal data is processed in accordance with the data protection principles and gives individuals rights to access, correct and control how the **Club** uses **Personal Data**.

5 Outline

5.1 The main themes of the Data Protection Laws are:

5.1.1 Good practices for handling **Personal Data**.

5.1.2 Rights for persons in respect of **Personal Data** that a **Data Controller** holds on them.

5.1.3 Being able to demonstrate compliance with these laws.

5.2 In summary, Data Protection Law requires each **Data Controller** to:

5.2.1 Only process **Personal Data** for certain purposes.

5.2.2 Process **Personal Data** in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner).

5.2.3 Provide certain information to those individuals about whom the **Club** processes **Personal Data,** which is provided in a privacy notice which individuals will have received from the **Club** as a member.

5.2.4 Respect the rights of those individuals about whom the **Club** processes **Personal Data** (including providing them with access to the **Personal Data** that the **Club** holds on them).

5.2.5 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.

5.3 Every **Member** has an important role to play in achieving these aims: It is their responsibility, therefore, to familiarise themselves with this **Policy**.

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

6 Principles

6.1 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:

6.1.1 **Fair and Lawful**. Processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met.

6.1.2 **Purpose Limitation**. Collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes.

6.1.3 **Data Minimisation**. Adequate and relevant, and limited to what is necessary to the purposes for which it is processed.

6.1.4 **Accuracy**. Data is accurate and where necessary kept up-to-date.

6.1.5 **Storage Limitation**. Kept for no longer than is necessary for the purpose.

6.1.6 **Integrity and Security**. Processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures.

7 Processing

7.1 For personal data to be processed lawfully, the **Club** must be processing it on one of the legal grounds set out in the Data Protection Laws. For the processing of ordinary **Personal Data** in the **Club**'s organisation these may include, among other things:

7.1.1 The data subject has given their consent to the processing (perhaps on their membership application form or when they registered on the club's website).

7.1.2 The processing is necessary for the performance of a contract with the **Data Subject** (for example, for processing membership subscriptions).

7.1.3 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).

7.1.4 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 Personal Data

8.1 Data will relate to an individual and therefore be their **Personal Data** if it:

8.1.1 Identifies the person. For instance, names, addresses, telephone numbers and email addresses.

8.1.2 Its content is specifically about the person. For instance, medical records, credit history, a recording of their actions, or contact details.

8.1.3 Relates to property of that person, for example their home, their car or other possessions.

8.1.4 It could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if it is possible to link the data to the individual to tell others something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant).

8.1.5 Is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of a club meeting this may not relate to the individual and may be more likely to relate to the organisation that they represent.

8.1.6 Has the individual as its focus; that is the information relates to the individual personally rather than to some other individual or a transaction or an event that they were involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to that person.

8.1.7 Affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address, or location and work email addresses can also be personal data.

8.1.8 Is an expression of opinion about the person.

8.1.9 Is an indication of the Club's (or any other individual's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

8.2 Information about companies or other legal persons who are not a living persons is not **Personal Data**. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often **Personal Data**, so business related information can often be personal data.

8.3 Examples of information likely to constitute **Personal Data**:

8.3.1 Unique names.

8.3.2 Names together with email addresses or other contact details.

8.3.3 Job title and employer (if there is only one individual in the position).

8.3.4 Video and photographic images.

8.3.5 Information about individuals obtained as a result of Safeguarding checks.

8.3.6 Medical and disability information.

8.3.7 CCTV images.

8.3.8 Member profile information (e.g. marketing preferences).

8.3.9 Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

8.4 A full list of the Personal Data collected, stored and processed by the Club is shown at Annex A.

9 Special Category Personal Data

9.1 Under the Data Protection Laws **Personal Data** that relates to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data is known as **Special Category Personal Data**.

9.2 Previously **Special Category Personal Data** was referred to as "sensitive personal data" and some people may continue to use this term.

9.3 Under Data Protection Laws criminal records history becomes its own special category which is treated for some parts the same as **Special Category Personal Data**.

9.4 To lawfully process **Special Category Personal Data** the **Club** 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:

9.4.1 The processing is necessary for the performance of the **Club**'s obligations under employment law.

9.4.2 The processing is necessary to protect the vital interests of the **Data Subject**. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation.

9.4.3 The processing relates to information manifestly made public by the **Data Subject**.

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

9.4.5 The processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

9.5 To lawfully process **Special Category Personal Data** relating to criminal records and history the **Club** must either ensure that:

9.5.1 The individual has given their explicit consent to the processing,

or

9.5.2 The **Club**'s processing of those criminal records history is necessary under a legal requirement imposed upon the **Club**.

9.6 The **Club** would normally only expect to process **Special Category Personal Data** or criminal records history data usually in the context of individuals for monitoring performance, drug and alcohol testing, health and safety requirements, safeguarding checks, etc.

9.7 A full list of the Personal Data collected, stored and processed by the Club is shown at Annex A.

10 Processing Personal Data

10.1 Virtually anything the **Club** does with **Personal Data** is processing including collection, modification, transfer, viewing, deleting, holding, backing-up, archiving, retention, disclosure or destruction. So even just storage of **Personal Data** is a form of processing. The **Club** might process personal data using computers or manually by keeping paper records.

10.2 Examples of processing **Personal Data** might include:

10.2.1 Using personal data to correspond with members;

10.2.2 Holding **Personal Data** in the **Club**'s databases or documents.

10.2.3 Recording **Personal Data** in personnel or member files.

10.3 A full list of the Personal Data collected, stored and processed by the Club is shown at Annex A.

11 Data Subject Rights

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

11.1.1 Access their personal data; usually referred to as a subject access request.

11.1.2 Have their personal data rectified.

11.1.3 Have their personal data erased, usually referred to as the right to be forgotten.

11.1.4 Restrict processing of their personal data.

11.1.5 Object to receiving direct marketing materials.

11.1.6 Portability of their personal data.

11.1.7 Object to processing of their personal data.

11.1.8 Not be subject to a decision made solely by automated data processing.

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 the **Club** (if the **Club** is the relevant data controller) 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, taking into account the complexity and number of the requests. The **Club** 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 form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

11.4 If the **Club** receive the request from a third party (e.g. a legal advisor), the **Club** 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. This will usually mean contacting the relevant individual directly to verify 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 the **Club** has not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make the **Club** comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in the **Club**'s case will usually be the ICO.

11.7 In addition to the rights discussed in this document, any individual 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. The ICO must investigate and may serve an "Information Notice" on the **Club** (as the **Data Controller**). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to the Club Secretary from the ICO.

11.8 In the event of any **Member** receiving such a notice, they must immediately pass the communication to the Club Secretary.

12 Notification and Response

12.1 If any **Member** receives a request (in whatever form - verbally, in writing, by e-mail or via any social media) or believes they have a request for the exercise of a **Right**, they should pass the message, letter, e-mail, tweet or Facebook entry to the Club Secretary.

12.2 The Club Secretary should:

12.2.1 Log receipt of the request and record all relevant details, explain the procedure as required, and get the request confirmed in writing if necessary.

12.2.2 Inform the other members of the **Data Protection Working Group** (see Section 3) of the request.

12.2.3 Having consulted with other members of **Data Protection Working Group** respond to the **Data Subject** on the **Club**'s behalf confirming formal receipt of the request.

12.3 Members of the **Club**'s **Data Protection Working Group** will consider the **Club**'s response: The action taken will depend upon the nature of the request. The **Data Protection Working Group** will write to the individual and explain the position, and the legal situation including any external legal advice if necessary, and whether the Club will comply with the request. A standard letter/email from should suffice in most cases.

12.4 The **Data Protection Working Group** will co-ordinate any additional activity required to meet the request, inform any relevant **Member** of any action that must be taken as a result of the request.

13 Members' Obligations

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

13.1.1 Treat all personal data with respect.

13.1.2 Treat all personal data how individuals would want their own personal data to be treated.

13.1.3 Immediately notify the Club Secretary, or any other member of the **Data Protection Working Group,** 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.

13.1.4 Take care with all personal data and items containing personal data they handle or come across so that it stays secure and is only available to or accessed by authorised individuals.

13.1.5 Immediately notify the Club Secretary, or any other member of the **Data Protection Working Group,** if they become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this see the **Club**'s separate Data Breach Policy which applies to all of the **Members** regardless of their position or role in the **Club**'s organisation.

14 Members' Activities

14.1 Data protection laws have different implications in different areas of the **Club**'s organisation and for different types of activity, and sometimes these effects can be unexpected.

14.2 Areas and activities particularly affected by data protection law include human resources, payroll, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

14.3 The **Club** must consider what personal data individual **Members** might handle, consider carefully what data protection law might mean for those individuals and their activities, and ensure that those individuals comply at all times with this **Policy**.

15 Practical Matters

15.1 Personal data should only be accessed and seen by those who need to see it. Whilst **Members** should always apply a common sense approach to how individuals 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 Do not take personal data out of the organisation's premises (unless absolutely necessary).

15.1.2 Only disclose unique logins and passwords to authorised people and not to anyone else.

15.1.3 Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

15.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on their drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

15.1.5 If staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when not needed.

15.1.6 Do encrypt laptops, mobile devices and removable storage devices containing personal data.

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

15.1.8 Do password protect documents and databases containing personal data.

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

15.1.10 When picking up printing from any shared printer always check to make sure individuals only have the printed matter that individuals expect, and no third party's printing appears in the printing.

15.1.11 Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

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

15.1.13 When in public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device displaying personal information. If necessary move location or change to a different task.

15.1.14 Do ensure that their screen faces away from prying eyes when processing personal data. Do challenge unexpected visitors or individuals accessing personal data.

15.1.15 Do not leave personal data lying around: Store it securely.

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

15.1.17 If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information that may identify that individual to others who may overhear in a similar way to if individuals were speaking on the telephone.

15.1.18 Never act on instructions from someone unless individuals are absolutely sure of their identity and if individuals are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

15.1.19 Do not transfer personal data to any third party without prior written consent of **Data Protection Working Group**.

15.1.20 Do notify the Club Secretary, or any other member of the **Data Protection Working Group,** immediately of any suspected security breaches or loss of personal data.

15.1.21 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the Club Secretary, or any other member of the **Data Protection Working Group**. For more details on this see the **Club**'s separate Data Breach Policy which applies to all the **Club Members** regardless of their position or role in the **Club**'s organisation.

15.2 Whatever, individuals should always take a common sense approach, and if **Members** see any areas of risk that they think are not being addressed then bring the matter to the attention of any member of the **Data Protection Working Group**.

16 Foreign Transfers of Personal Data

16.1 Personal data must not be transferred outside the European Economic Area (EEA) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of **Personal Data** or the **Club** has put in place adequate protections.

16.2 This is mainly relevant to **Personal Data** held and accessed in Cloud-based services as well as data processing the **Club** may outsource.

16.3 These protections may come from special contracts the **Club** need to put in place with the recipient of the **Personal Data**, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection.

16.4 Under no circumstances can any **Personal Data** be transferred outside of the EEA without the prior written consent of the **Data Protection Working Group**.

16.5 The **Club** will also need to inform **Data Subjects** of any transfer of their **Personal Data** outside of the UK and may need to amend the privacy notice to take account of the transfer of data outside of the EEA.

17 Breach of Policy.

17.1 Any breaches of this **Policy** will be viewed very seriously. All **Members** must read and implement this **Policy** carefully and make sure that they are familiar with it. Breaching this **Policy** is a disciplinary offence and will be dealt with under the **Club**'s Disciplinary Procedure.

17.2 If individuals do not comply with Data Protection Laws and/or this **Policy**, then **Members** are encouraged to report this fact immediately as explained in Section 13. 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.

17.3 Also if **Members** are aware of or believe that any other representative of the **Club** is not complying with Data Protection Laws and/or this **Policy**, then they should report it in confidence to the Club Chairman, or any other member of the **Data Protection Working Group**.

17.4 There are a number of serious consequences for individual **Members** if they do not comply with Data Protection Laws. These include:

17.4.1 **Investigations and interviews**: Individual **Members'** actions could be investigated and they could be interviewed in relation to any non-compliance.

17.4.2 **Disciplinary action:** Where individuals are a volunteer, failure to comply with the **Club**'s policies could lead to termination of their membership and/or volunteering position with the **Club**. If individuals are an employee, their terms and conditions of employment require them to comply with the **Club**'s policies. Failure to do so could lead to disciplinary action including dismissal.

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

17.5 There are a number of serious consequences for the **Club** it does not comply with Data Protection Laws. These include:

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

17.5.2 **Assessments, investigations and enforcement action**: The **Club** could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

17.5.3 **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of the **Club**'s non-compliance.

17.5.4 **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage the **Club**'s reputation. Court proceedings are public knowledge.

17.5.5 **Loss of Reputation:** Prospective members, participants, players, customers, suppliers and contractors might not want to deal with the **Club** if the **Club** are viewed as careless with personal data and disregarding the **Club**'s legal obligations.

17.5.6 **Civil Fines:** These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher.

17.5.7 **Court Orders**: These may require the **Club** to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

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

18 Queries

18.1 If individuals have any queries about this Policy please contact any member of the **Data Protection Working Group**.

ANNEX A

Personal Data (Information) Held on Club Database (by FullOnSport)

1.1 Title

1.2 First Name

1.3 Last Name

1.4 Gender

1.5 Date of Birth

1.6 Full Address

1.7 Email Addresses (Primary and Secondary)

1.8 Telephone Numbers (Primary and Secondary)

1.9 Team

1.10 Training Group

1.11 Team Shirt Number

1.12 School

1.13 School Year

1.14 Ethnicity

1.15 Disability

1.16 Emergency Contact Name

1.17 Emergency Contact Telephone Number

1.18 Medical Information