General Data Protection Regulation
Data Protection Act 2018

Issue 2

Issued: July 2023

INTRODUCTION

This Policy is to ensure that Hitchin Netball Club complies with the requirements of the General Data Protection Regulation, Data Protection Act 2018, and associated guidance and Codes of Practice issued under the legislation.

Hitchin Netball Club is committed to complying with data protection law and to respecting the privacy rights of individuals. The Policy applies to all of our staff, committee, volunteers, players and their family. (Throughout this document to be known for simplicity as the "team 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.

Data protection law is a complex area. 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.

1. 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 are not required to appoint a Data Protection Officer, if you have any questions regarding data protection please contact the Committee.

2. Why do we have a data protection Policy?

2.1 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 our members.

3. Status OF THIS Policy and the implications of breach.

3.1 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.

3.2 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the Committee. 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.

4. Other consequences

4.1 There are a number of serious consequences for both yourself and the club if we do not comply with Data Protection Laws. These include, disciplinary, criminal sanctions reputational risk and fines.

5. Data protection laws

5.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) and applies to any personal data that we process.

5.2 The Data Protection Laws all 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 (on which see below).

6. Key words in relation to data protection

6.1 **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 our possession). That living individual might be a player, member, parent, volunteer or Committee member, and that personal data might be written, oral or visual (e.g. CCTV).

6.2 **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 us (e.g. a job title and company name).

6.3 **Data subject** is the living individual to whom the relevant personal data relates.

6.4 **Processing** is widely defined under data protection law and 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.

6.5 **Data controller** is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our members.

6.6 **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, for example an outsourced payroll provider will be a data processor.

7. Personal data

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

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

7.1.2 its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;

7.1.3 relates to property of the individual, for example their home, their car or other possessions;

7.1.4 it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you 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);

7.1.5 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 an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;

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

7.1.7 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;

7.1.8 is an expression of opinion about the individual; or

7.1.9 is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

7.2 Examples of information likely to constitute personal data:

7.2.1 Unique names;

7.2.2 Names together with email addresses or other contact details;

7.2.3 Job title and employer (if there is only one person in the position);

7.2.4 Video - and photographic images;

7.2.5 Information about individuals obtained as a result of Safeguarding checks;

7.2.6 Medical and disability information;

7.2.7 CCTV images;

7.2.8 Member profile information (e.g. marketing preferences); and

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

8. Lawful basis for processing

8.1 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.

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

8.2.1 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)

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

8.2.3 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

8.2.4 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).

9. Special category data

9.1 Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

9.2 Under Data Protection Laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

9.3 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:

9.3.1 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 another extreme situation;

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

9.3.3 the processing is necessary for the purpose of establishing, exercising or defending legal claims; or

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

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

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

10. When do we process personal data?

10.1 Virtually anything we do 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. We 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 our databases or documents; and

10.2.3 Recording personal data in personnel or member files.

11. Outline

11.1 The main themes of the Data Protection Laws are:

11.1.1 good practices for handling personal data;

11.1.2 rights for individuals in respect of personal data that data controllers hold on them; and

11.1.3 being able to demonstrate compliance with these laws.

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

11.2.1 only process personal data for certain purposes;

11.2.2 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);

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

11.2.4 respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and

11.2.5 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.

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

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

12. Data protection principles

12.1 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:

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

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

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

12.1.4 accurate and where necessary kept up to date;

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

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

13. Notification and response procedure

13.1 If a member has a request or believes they have a request for the exercise of a right to access and understand the personal information the Club holds on them, they should pass this on to the Committee who will then respond to the data subject.

14. Your main obligations

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

14.1.1 Treat all personal data with respect;

14.1.2 Treat all personal data how you would want your own personal data to be treated;

14.1.3 Immediately notify the Committee 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;

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

14.1.5 Immediately notify the Committee if you become aware of or suspect the loss of any personal data or any item containing personal data.

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 Only disclose your unique logins and passwords for any IT systems to authorised personnel and not to anyone else.

15.1.2 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.

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

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

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

15.1.6 Do password protect documents and databases containing personal data.

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

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

15.1.9 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.

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

15.1.11 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 you are using when you have personal information on display. If necessary move location or change to a different task.

15.1.12 Do ensure that your screen faces away from prying eyes if you are processing personal data. Personal data should only be accessed and seen by those who need to see it.

15.1.13 Do challenge unexpected visitors or employees accessing personal data.

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

15.1.15 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.

15.1.16 If taking down details or instructions in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

15.1.17 Never act on instructions from someone unless you are absolutely sure of their identity and if you 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.

15.1.18 Do not transfer personal data to any third party without prior written consent of the Committee.

15.1.19 Do notify the Committee immediately of any suspected security breaches or loss of personal data.

15.1.20 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our Committee.

15.2 However you should always take a common-sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of our Committee.