DATA PROTECTION POLICY

Awareness of GDPR

GDPR is the General Data Protection Regulation, the new EU - wide data protection legislation which comes into force on 25th May 2018.
The Association committee shall ensure that all committee members and Association volunteers are aware of the Association's obligations under GDPR, with particular emphasis on what to do in the case of a data breach and how to hold and process data securely. This shall be achieved by an introductory session upon introduction, and then subsequently it shall always be covered at the start of every new committee year.

Data Holding Policy

The Association shall make all reasonable efforts to hold data only electronically and in a structured form e.g.
in a password protected database. All other forms of unstructured data retention such as printed copies or stored electronically on personal devices need to be kept to a minimum.
The aim is to make it as easy as possible for the Association to identify, locate, and control data held by the Association.
The Association will hold personal data for the following lengths of time dependant on the circumstances:

Circumstance	Lawful basis	Period of time	Action after period
Current member data	Consent	2 years	Deletion
Umpire data	Legitimate interest	2 years	Deletion
Coach / volunteer	Legitimate interest	2 years	Deletion
DBS checks	Legal obligation	1 year	Deletion
Email files	Legitimate interest	2 years	Deletion
General hard copies	Legitimate interest	2 years	Deletion

The Association shall keep a record of its holding and processing of personal data. This shall be initially populated following a Data Audit performed as soon as practically possible before 25th May 2018.

Data Protection Impact Assessments (DPIAs)

DPIAs need to be performed whenever the Association adopts a new technology that involves processing personal data, or when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals.

Lawful Basis for Processing

The Association will ensure that it has a lawful basis for processing data before doing so. The lawful basis set out in the GDPR are:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests
- For the purposes of the Policy we do not consider it likely that we will need to use Vital Interest nor Public Task as lawful basis, so they will not be covered by this Policy.

DATA PROTECTION POLICY

Lawful Basis - Consent
When the Association wishes to use this as the lawful basis for processing personal data then it
shall ensure that the following rules are adhered to:

- The person has to positively opt in
- The consent needs to be granular and specific
- Consent needs to be separate from other terms, conditions, or policies the person is
- agreeing to
- The following information needs to be captured and retained about the consent:
- Who consented
- When they consented
- How they consented
- What they were told
- Proof of consent will need to be stored securely.

Lawful Basis –Contract
When the fulfilment of a contract requires the processing of personal data then this can be used as the lawful basis.

Lawful Basis – Legal Obligation
In carrying out its legal obligations the Association will need to process personal data. It will do so by hold and processing the minimum required data for the minimum required period. Legal obligations that we are aware of are:

- DBS Checks

Lawful Basis – Legitimate Interest
If the aforementioned lawful bases don't apply, then the Association shall use a Legitimate Interest Assessment to evaluate whether the data can be held and processed. This shall be done using the LIA form Annex B. If this can't be done, then the data shall be deleted.

Handling People's Rights
Data subjects have a set of eight rights with regards to their personal data.
Requests related to these rights shall be handled within a month of the request and shall be free of charge in so far as the request is reasonable and not
repetitive; in such instances then the Association may charge a fair administration fee proportionate to the work required.

Handling a Data Breach
A data breach is defined as: a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. As soon as a data breach a as discovered then a Data Breach Assessment needs to be performed to assess whether the Information Commissioner's Office (ICO) needs to be informed. If this is the
case, then this needs to be done with 72 hours of the data breach.
Telephone: 0303 123 1113,
Website: https://ico.org.uk/for-organisations/report-a-breach/
All committee and volunteers in the Association need to be acutely aware of this obligation and need to be held accountable to act upon it.

DATA PROTECTION POLICY

Handling of Special Category data

The Association is aware that is holds special category data and will ensure this is handled at the highest level of security as possible. The main types of special category data are:

- DBS checks
- Medical Conditions
- Juniors' Data

Security

The Association will secure data in line with the level of risk posed to the rights and freedoms of the data subjects.

On a general basis the following will be done to maintain a base level of security for all data:

- All devices holding or that provide access to personal data shall be password (or equivalent) protected.
- Destruction of hard copies shall be via a shredder
- The use of portable storage devices should be avoided, and where not avoidable such devices need to have password protection and encryption.

Where is Association membership data held?

We use Mailchimp to send out communications, which stores email addresses only.

We use the England Hockey Player Pathway System for those members in the Development and Academy system

Both systems are password protected using individual accounts specific to the relevant and limited number of Committee Members.

Some data is held on devices used by Committee Members such as mobile phones, laptops, and PCs. We have a policy to keep this to a minimum and for practical purposes only. All devices are required to be password protected. We will never hold sensitive data, or "risky" data such as credit card details, or details of people's medical conditions on such devices.

Some data is held in a physical format such as a paper form, as far as is reasonably possible we will endeavour to digitise this data. After digitisation the paper form will be shredded.

What rights do members have with regard to their data?

In accordance with the General Data Protection Regulation you have the following rights with regard to your personal data if you are situated within the EU. More information about these rights is available on the Information Commissioner's Office website:

www.ico.org.uk

The right:

- to be informed. This is all about transparency, so you know what data an organisation holds and what it is doing with it. This policy seeks to fulfil this right.
- to access. This enables you to see the exact data held by an organization.
- to rectification. This entitles you to force an organization to make corrections to the data held on you.
- to erase. This is also known as the right to be forgotten, and enables you force the complete deletion of your data as long as the organisation doesn't have lawful basis for holding and processing your data.
- to restrict processing. This is enables you to force an organisation to stop processing your data in a way.
- to data portability. This means the organisation is obliged to give you your data in an easy to transfer manner.

- to object. This means you have the right to object to the holding or processing of your data.
- in relation to automated decision making and profiling. This enables you to request that a human reviews the outcome of automated processing performed by a computer.

You can make a request to the Association at any time and we will respond as soon as we can and at the latest within one month of the request. As long as the request is reasonable and not repetitive we will not change anything for such requests. If the request is unreasonable or repetitive then we will change a fair administration fee proportionate to the amount of work involved, and this will be made known to the individual before conducting the work.

If you wish to lodge a complaint against us, you can do this with the ICO (www.ico.org.uk).

What happens if something goes wrong?
A data breach is defined by the GDPR as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If we experience a data breach, we will first assess the severity of the breach and decide whether
the breach warrants informing the ICO, this will be done within 72 hours of the breach. If necessary, you will be contacted.