Personal Data Protection

Club wide awareness of GDPR

The Club committee shall ensure that all committee members and club volunteers are aware of the Club'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 (for the first time in 2018), and then subsequently it shall always be covered at the start of every new committee year.

Data Holding Policy

The Club shall make all reasonable efforts to hold data only electronically and in a structured form e.g. on a password protected database. All other forms of unstructured data holding need to be kept to a minimum e.g. keeping hard copies, keeping files stored on personal devices. The aim is to make it as easy as possible for the Club to identify, locate, and control data held by the Club.

The Club 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	1 year	Deletion
"Friends of" Data	Legitimate Interest	5 Years	Deletion
Umpire Data	Legitimate Interest	3 years	Deletion
Sponsor Data	Legitimate Interest	3 years	Deletion
Coach and Volunteer DBS Checks	Legal Obligation	1 Years after contract/volunteering ends	Deletion
Email Files	Legitimate Interest	2 Years	Deletion
General hard copies e.g. letters	Legitimate Interest	2 years	Deletion

Data Holding Awareness

The Club shall keep a record of its holding and processing of personal data. This shall be initially populated following a Data Audit performed before 25th May 2018, then annually reviewed in May. This may also be updated on an ongoing basis as and when applicable.

This shall be captured in the Data Holding and Processing Register.

Data Protection Impact Assessments (DPIAs)

DPIAs need to be performed whenever the Club 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.

The DPIA form is in Annex A.

Lawful Basis for Processing

The Club 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.

Lawful Basis - Consent

When the Club 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 Club 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 Club 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 Club may charge a fair administration fee proportionate to the work required. Details of People's Right to be Informed can be found in Annex C.

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 is discovered then a Data Breach Assessment (Annex D) 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 Club need to be acutely aware of this obligation and need to be held accountable to act upon it.

Handling of Special Category data

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

On a general bases 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.

Annex A – Data Protection Impact Assessment (DPIA)

Date Carried Out		By whom	
DPIA Title			
Describe the processing operations and the purposes (include a diagram of the data flow)			
Assess the necessity and proportionality of the processing in relation to the purpose. i.e. Do we have to do it this way?			
Assess the risks to the rights and freedoms of individuals i.e. what could happen if something went wrong? Consider the threats to the data and therefore the vulnerabilities. Rank risk severity and likelihood on a scale of 1-3 and times the two together. Levels 1 & 2 don't require any special attention above and beyond the everyday measures that the company takes. Levels 3 & 4 represent a moderate risk and sensible and considered action needs to be taken to address these risks. Levels 6 & 9 represent a high risk, and decisive action needs to be taken to mitigate these risks, if this can't be done then processing of the should not be carried out. Keep in mind impacts of: Inaccuracy, Keeping data too long, keeping too much data, unauthorised access, and disclosure to the wrong people.			
What measures will be put in place to address these risks? How will these measures be controlled?			
Created by			
Checked by Data Protection Officer (or nominee)			

Annex B – Legitimate Interest Assessment (LIA)

Date Carried Out		By whom	
General Description of data processing			

Purpose Test "Are you pursuing a legitimate interest?"

1. Why do you want to process the data – what are you trying to achieve?

2. Who benefits from the processing? In what way?

3. What would the impact be if you couldn't go ahead?

4. Would your use of the data be unethical or unlawful in any way?

The Necessity Test "Is the processing of data necessary for that purpose?"

1. Does this processing of data actually help to further the above Purpose?

2. Is it a reasonable way to go about it?

3. Is there another less intrusive way to achieve the same result?

The Balancing Test "Do the individual's interests override the legitimate interest?" 1. What is the nature of your relationship with the individual? 2. Is any of the data particularly sensitive or private? 3. Would people expect you to use their data in this way? 4. Are you happy to explain it to them? 5. Are some people likely to object or find it intrusive? 6. What is the possible impact on the individual? 7. How big an impact might it have on them? 8. Are you processing children's data? 9. Are any of the individuals vulnerable in any other way? 10. Can you adopt any safeguards to minimise the impact? 11. Can you offer an opt-out?
Created by
Checked by Data Protection Officer (or nominee)

Annex C – Right to be informed

Right to be informed – Data subjects have the right to know what of their personal data the Club holds and how it is processed.

Who's holding your data?

Your data is being held, processed, and controlled by:

Yate Hockey Club

mail@yatehockey.com

What data do we hold, and what are we doing with your data?

Depending on how you came into contact with the Club and what your ongoing relationship with the Club is, we will be holding and processing your data for different periods and reasons. The following table details our policy with regard to the different types of data and different types of interactions we might have with you.

Interaction	Data Held	Period Held	Processing	Purpose	Lawful Bases
Current Club Members	Name, contact details, date of birth, medical conditions	1 Year	Membership, Club communication	To be able to ensure member information is up to date and keep you updated with Club news	Consent
"Friends of Yate Hockey"	Name, Email Address	Up to 5 years without interaction with our Club.	Club communication	To be able to keep you updated with Club news	Legitimate interest
Umpires	Name, Email address, Contact Number	Up to 3 years without interaction with our Club	Club communication, Officiating opportunities	To be able to keep you updated with Club news, make you aware of officiating opportunities	Legitimate interest
Sponsors	Name, Contact Details	Up to 3 years without interaction with the Club	Club communications, sponsorship opportunities	To be able to keep you updated with Club news, make you aware of sponsorship opportunities	Contract, Legitimate Interest

Coaches/ Volunteers	Name, Contact Details, DBS Information	Up to a year after coaching/ volunteering ends	Club Communications, Legal requirements	To be able to keep you updated with Club news, fulfil our legal requirements	Contract, Legal Obligation

Where is my data held?

We use MailChimp to send out Club communications, which stores Names and Email Addresses only. The Club account is password protected and a select number of Committee Members have access to the account.

We also use Google Drive to store Data in spreadsheets, Word files, PDFs, etc. This account is password protected and only accessible by 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. Unless of course you send this data in an email, in which case it will remain on devices for a period of time until it can be stored elsewhere in a more secure fashion.

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.

We, as a Club, have a policy of deleting emails after 2 years.

What rights do I have with regard to my 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 a 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 enables you to force an organisation to stop processing your data in a particular 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 Club 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?

If we experience a data breach, as defined by the GDPR as: a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Then 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 contacted.

Annex D – Data Breach Assessment

Form Date	
Date of Breach	
Description	
Assessment of volume (of data) and severity (to data subjects)	
Does the ICO need to be informed?	YES / NO if Yes: Done on date: Ref no:
Form completed by	Name: