Easthampstead Golf Club

Privacy Impact Assessment

EGC/REP/PIA/001

21 September 2020

Version: 1.3

Authorisation Record			
Author Name	Chris Corbett	Approver Name	Club President
Signature		Signature	
Date		Date	

DISTRIBUTION LIST

Number	Copy To	Location
1	Rod Clay	rod_clay@live.com
2	Matthew Irving	mp.irving@gmx.com
3	Steve Cross	sdvc101@outlook.com
4	George Friedman	george.friedman@btinternet.com
5	Dean Pullen	dpullen@movetech.co.uk
6	Sean Wheatley	seanwheatley@hotmail.co.uk
7	Stephen Eddy	ehgcmembers@stepheneddy.com
8	Ian Nicholson	nickianking@aol.com
9	Richard Gater	gater933@gmail.com
10	Ted Rogers	ted.rogers@btinternet.com

CHANGE HISTORY

Date	Version	Summary of Change	Author
26/01/2018	0a	First draft for internal committee review.	Chris Corbett
09/02/2018	0b	Second draft after initial review.	Chris Corbett
12/02/2018	0c	Updated to follow GDPR Principles more closely.	Chris Corbett
01/03/2018	0d	Included paper forms and information retained on juniors.	Chris Corbett
06/03/2018	0e	Updates following review and to account for changes in the Junior membership form where medical details collected has changed.	Chris Corbett
14/03/2018	1	Formal release version following committee consideration of last risk issues.	Chris Corbett
03/04/2018	1.1	Clarifications on status of Data Processors	Chris Corbett
13/06/2019	1.2	Annual review. Minor changes only. Data collected has not changed.	Chris Corbett
21/09/2020	1.3	Annual review. Updated privacy notice to include England Golf words, a change driven by the introduction of the World Handicap System.	Chris Corbett

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

The purpose of this document is to record the details of a Privacy Impact Assessment (PIA) on the data held by Easthampstead Golf Club (EGC) on behalf of its members. A PIA is a recommended approach by the Information Commissioner's Office to allow an organisation to identify the most effective way to comply with their data protection obligations. This document closely follows the recommended layout and contents for a PIA.

The scope of this document includes the members' data that is held on the club's website and data collected on application forms for membership either as an adult or a junior player.

This PIA has been produced in the light of new data protection legislation that became law in the UK on 25 May 2018 – the General Data Protection Regulation (GDPR).

1.2 Reference Material

[1] Overview of the General Data Protection Regulation (GDPR), Information Commissioner's Office, Oct 2017, Version 1.13.4.

[2] Conducting privacy impact assessments – code of practice, Information Commissioner's Office, Feb 2014, Version 1.0.

1.3 Glossary and Abbreviations

CISPE	Cloud Infrastructure Service Providers in Europe
DPA	Data Protection Act
EGC	Easthampstead Golf Club
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IP	Internet Protocol
ISO	International Standards Organisation
IT	Information Technology
PIA	Privacy Impact Assessment

1.4 Location of Text

Electronic: Website: Documents

Hardcopy: N/A

2. Identifying the Need for a PIA

The club website has been in existence for several years, but over that time no formal activity to assess data held on the site and risks to it has been undertaken.

Paper records of membership application are retained by the club that contains additional information to that recorded on the website. Management of these paper records has also not previously been assessed for data protection risks.

Given the imminent arrival into UK law of the GDPR with more stringent requirements on data protection, it has been deemed prudent to perform a formal privacy impact assessment.

The result will be an accurate record of data held by the club about its members, the perceived risks to that data, and a statement of how the data protection principles are applied by the club.

3. Data Definition and Information Flows

3.1 Club Website

The information in Table 1 identifies the exact types of personal data that are collected by EGC and stored within the website database. Contents of this table in association with the user interactions and data flows next provides a complete specification of personal data managed by the club on its website. Note that accounts on the website include men, juniors and ladies' members.

Data Id	Data Name	Data Type	Storage	Retention
1	Members Full Name	Text	Database Table	Member lifetime
2	e-mail address	Text	Database Table	Member lifetime
3	Home telephone number	Number	Database Table	Member lifetime
4	Mobile telephone number	Number	Database Table	Member lifetime
5	Password	Encrypted text	Database Table	Member lifetime
6	Internet Protocol (IP) Address	4-octet string	Audit Log	1 year

Table 1 Personal Data Stored on EGC Website

A set of these data items is stored for each member of the club who has registered on the website, which at the time this document was created was 352 but is never likely to exceed 400.

Data acquisition for Data Ids 1 to 5 is performed directly by the individual concerned. Each data item is collected by a data entry form that is part of the registration process implemented on the website.

Data for Id 6 in the table is collected in an audit log automatically. Data in the audit log is retained for a year and is used to produce website usage reports and to assist in identifying security breaches, specifically where unregistered individuals may be attempting access to the site.

The lifecycle for this data is depicted in Figure 1, which illustrates the major stages by which the data is created, managed, used and deleted. For each major stage the figure provides a summary of the user interactions that are possible with the data.

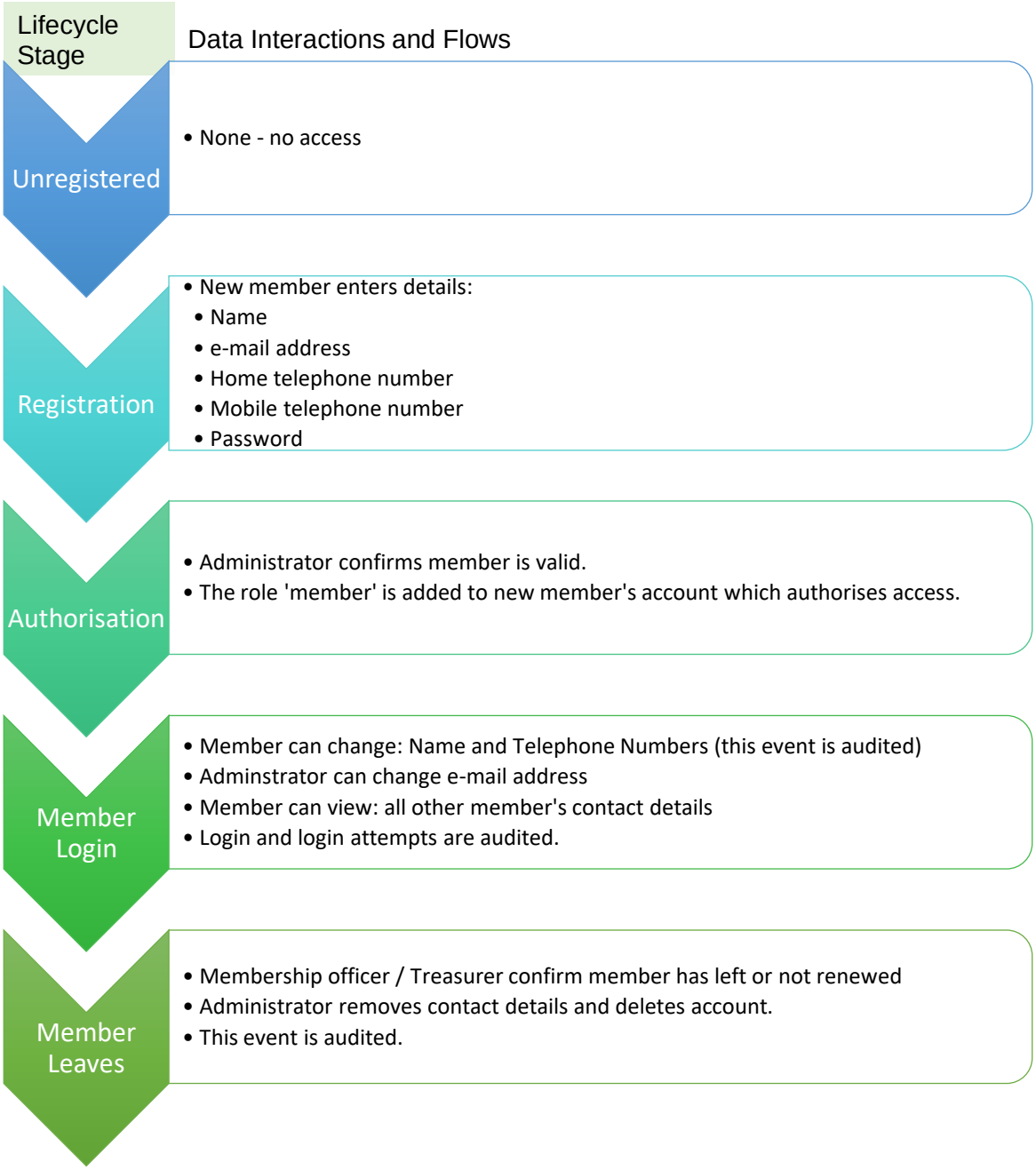

Figure 1 Data Lifecycle on EGC Website

3.2 Paper/Online Application Forms

In order to become a member of the club, minimum details are required to register the new member, maintain contact with them and, importantly for golf, manage handicaps. These details are collected in one of two ways:

1. Completing an online application form and delivering by email to the Member Secretary of the Club. While filling a form online the connection used is encrypted for confidentiality.

2. Completing a paper application form and sending by post to the Member Secretary.

In both cases the data set collected is as shown in Table 2 below.

Id	Data Name	Data Type	Storage	Retention
1	Members Full Name	Text	Printed Paper Form	Member Lifetime
2	Postal Address	Text	Printed Paper Form	Member Lifetime
3	Date of Birth	Text	Printed Paper Form	Member Lifetime
4	Home Telephone Number	Number	Printed Paper Form	Member Lifetime
5	Mobile Telephone Number	Number	Printed Paper Form	Member Lifetime
6	E-mail Address	Text	Printed Paper Form	Member Lifetime
7	Sponsor	Text	Printed Paper Form	Member Lifetime
8	Current Handicap (CDH)	Number	Printed Paper Form	Member Lifetime

Table 2 Data Collected on Paper or Online Application Forms

There are some items above that are additional to website account registration.

Item 3, data of birth, is required to classify the member into the senior's category for competition eligibility purposes.

Item 7, Sponsor, is the name of an existing member of the Club who is sponsoring the applicant for membership.

Finally, item 8 is needed so that the new member can provide his current handicap at the time of application or has no handicap and will await assignment by the club under the appropriate rules.

These additional items assist in registering the member on Handicap Master (a cloud service) for maintenance of their handicap.

Paper applications and printed copies of online applications are retained in a folder by the Member Secretary. On confirmation that a member has left the club, the Member Secretary will shred the relevant application form.

3.3 Information Related to Junior Members

The Club maintains a popular junior's section for young people under 18. Information requested from junior members is more extensive than that collected for adult members and does include more sensitive medical information. For a junior applicant, data is collected on paper forms only and not online. The application form collects data in two parts as described in the two tables below.

First, Table 3 below defines the data collected for contact and handicapping purposes.

Id	Data Name	Data Type	Storage	Retention
1	Juniors Full Name	Text	Paper	Member Lifetime
2	Postal Address	Text	Paper	Member Lifetime

Id	Data Name	Data Type	Storage	Retention
3	Date of Birth	Text	Paper	Member Lifetime
4	Contact telephone number	Number	Paper	Member Lifetime
5	Parent's telephone number	Number	Paper	Member Lifetime
6	Parent's mobile number	Number	Paper	Member Lifetime
7	Parent's email address	Text	Paper	Member Lifetime
8	Alternative Contact name	Text	Paper	Member Lifetime
9	Alternative contact number	Number	Paper	Member Lifetime
10	Home Club	Text	Paper	Member Lifetime
11	Current handicap (CDH)	Number	Paper	Member Lifetime

Table 3 Membership Data Collected on Junior Members

Data that is collected related to a Junior member's medical status is described in Table 4 below.

Id	Data Name	Data Type	Storage	Retention
1	Doctors name	Text	Paper	Member Lifetime
2	Doctor's Surgery Address	Text	Paper	Member Lifetime
3	Doctor's Surgery Telephone Number	Text	Paper	Member Lifetime
4	Medication Required	Yes/No	Paper	Member Lifetime
5	Medication Details	Text	Paper	Member Lifetime
6	Allergies	Yes/No	Paper	Member Lifetime
7	Allergy Details	Text	Paper	Member Lifetime
8	Dietary Requirements	Yes/No	Paper	Member Lifetime
9	Details of Diet	Text	Paper	Member Lifetime
10	Other Requirements	Yes/No	Paper	Member Lifetime
11	Description of additional needs	Text	Paper	Member Lifetime
12	Disability	Yes/No	Paper	Member Lifetime
13	Details of Disability	Text	Paper	Member Lifetime
14	Communication Needs	Yes/No	Paper	Member Lifetime
15	Communication Details	Text	Paper	Member Lifetime

Table 4 Medical Data Collected on Junior Members

The completed junior membership form is retained in a restricted access folder in the office within the Pro-shop of the Downshire Golf Complex.

Access to this folder is defined under the club's policy for Safeguarding. The policy currently is that access is restricted to the Club Welfare Officer, the Junior Organiser, the Downshire Complex manager and the PGA Golf Professionals.

None of the medical data or membership data collected on these paper forms is transcribed to electronic form nor stored electronically.

Should a Junior member also wish to use the website (for which they are entitled to gain access to the playing calendar), then they separately register using the details described in Section 3.1.

3.4 Data Processors

The data listed in Table 1 is stored within a database as part of the club website hosted by Netcetera, a specialist hosting supplier.

The information set comprising Name, Date of Birth and email address is further provided to a hosted Handicap Management service provided by Handicap Master. These details are forwarded on to England Golf, whose IT Systems run the software that manages members Handicap Indexes as part of the World Handicap System.

None of the paper-based information is passed to any Data Processor.

4. Consultation Requirements

Data specifications and risks to that data presented in this document must be reviewed and agreed by the club committee and following review be signed off by the Club President on the area provided on the front page.

There are no specific requirements for an external review of this PIA, but the club committee may wish to consider providing copies to Bracknell Forest Council and, from March 2018, Sports and Leisure Management Ltd.

5. Privacy and Related Risks

This section presents the risks determined by the EGC committee to be those of significance to club members in relation to the data identified above.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Corporate Risk
1. Passwords exposed	Malicious website user may alter personal contact details or register real user for competitions causing some embarrassment and irritation. Real user may have chosen password common to other accounts, thus malicious user may gain access to more	If data is altered maliciously it is no longer accurate as required by the protection principles.	Maliciously altered contact details will cost club officials time in correcting data. Club could be subject to financial penalties if loss of passwords results in consequential loss of, for example, cash from a bank account.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Corporate Risk
	sensitive data such as real user's bank account.		
2. Contact details incorrect	Club member is not informed of events or changes to events such as competition tee times. Data on leaving members is not removed. Information pertinent to one individual may be incorrectly sent to another (for example, payment reminders or club disciplinary notifications).	Data is not being used in the manner for which it was submitted. Club may be in conflict with Principle 5, retention of data only for as long as necessary. Data is not accurate.	Club creates confusion and ill feeling amongst members.
3. Loss of member data in bulk	Data that is lost accidentally or through hacking maybe be used in a variety of ways to contact the member(s) affected for fraudulent purposes.	Bulk data loss is a significant breach of security and will require reporting to the ICO.	Club may be subject to uncomplimentary articles in the press. Club may be subject to action by members who suffer consequential loss. Club may be subject to fines.
4. Printing and copying of member contact details in bulk from website by a registered member.	Members contact data could be accidentally or deliberately released into the public and used by others for reasons not related to the golf club.	Bulk data loss is a significant breach of security and will require reporting to the ICO.	Club may be subject to uncomplimentary articles in the press. Club may be subject to action by members who suffer consequential loss. Club may be subject to fines.
5. Sensitive medical details of junior member's may be accidentally or deliberately released to	Release of health issues considered to be private by anyone would cause distress and potentially embarrassment.	The Club could be in breach of Principles 2 and 6 of the data protection regulations, whereby data is not being used	Club may be subject to uncomplimentary articles in the press. Club may be subject to action by members who suffer consequential loss.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Corporate Risk
unauthorised persons.		for the reasons it was submitted nor is it being protected adequately.	Club may be subject to fines.

6. Privacy Solutions

Risk	Solution(s)	Result	Evaluation
1	Ensure passwords are technically protected by: • Encrypting while in transit (using https) • Encrypting while stored on server	Passwords appear in the clear nowhere other than as user enters on keyboard. Industry standard public key cryptography relied upon to protect data in transit.	Risk of exposure by technical means lowered to minimum possible level using industry standard commercial methods. Users still need reminding of measures to protect their own passwords. Risk reduced.
2	Give member rights to modify their own data. Also provide rights to modify data to select small number of club officials for data management. Specific tasks include role management (role membership determines what data a member has access to), and bulk correction of data. Ensure website audit trail records when data is changed and by who.	Member in total control of accuracy of his / her own data. Club officials can police and audit data changes to ensure and monitor accuracy. Unexpected / unusual changes can be tracked in audit trail.	No documented process for the removal of member account details is in place. Risk reduced.
3	Ensure hosting provision for website is with an organisation that has appropriate Information Security standards with a recognised certification. Ensure handicap management service provider is cognisant of the	Club has confidence that measures to protect data stored on servers with both their data processors is commensurate with national or international standards.	Website provider has ISO270001 security certification. Website provider is assessing compliance to GDPR under CISPE code of conduct. Handicap Master publishes their

Risk	Solution(s)	Result	Evaluation
	responsibilities under the GDPR.		detailed responsibilities and compliance status to the GDPR on their website.
4	Consider removing bulk member contact detail display on website page (this function only available to authenticated and authorised members). Allow only single member searches.	Bulk data is not displayed on any site page. Does not prevent extraction of data (can be done one person at a time) but reduces risk by making it much more time consuming.	Data lost in bulk through normal web site functions may cause embarrassment to club. Risk reduced if display of all member contact details removed, otherwise risk accepted. A key feature of the club's holding of contact details is to allow members to contact others to arrange matches. Restricting this functionality could therefore be counter-productive for members and the club.
5	Restrict access to the sensitive data on Juniors. Never store medical data online or elsewhere, especially as it is only ever needed at the Golf Complex. Consider storing folder with Juniors data inside a combination lockbox so that the code is given only to those who need the access as defined by the Safeguarding policy.	Data cannot be obtained from an online leak. Only a small number of people have access.	Risk reduced with data retained only on paper. Enhancing security with a lockbox would reduce risk of breach but would also result in longer delays in accessing the data should it be urgently required as a result of a medical incident. Club committee need to determine least risk option.

7. Linking to Data Protection Principles

Within the current UK's Data Protection Act (DPA) there are eight guiding Principles against which an organisations compliance can be judged. In the GDPR, the first six principles are the same while the last two have been removed. What the table below provides is a statement of compliance by the EGC against each of the six guiding principles of the GDPR, while for completeness also provides a statement against the two additional DPA principles which are highlighted at the end of the table.

Principle	Requirement	Compliance Statement
1	Personal data shall be processed fairly and lawfully and with transparency.	A member consents to provide his or her contact details when registering for membership. The minimum information is supplied to allow the member to be contacted for the following purposes: 1. Arranging competition events at the home course and away 2. Supplying golf club news 3. Requesting membership renewals 4. Publicising club social events 5. Managing handicaps
2	Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.	Purposes for obtaining personal data are outlined under Principle 1. The data is never processed further. Junior's medical data cannot be 'processed' in any electronic sense.
3	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	The personal data has been refined to the absolute minimum required to allow meaningful and timely contact with the member. For example, postal addresses are not required or stored on the website. Junior's medical data is retained on paper in a secure location and accessed by only a few people.
4	Personal data shall be accurate and, where necessary, kept up to date.	The member alone enters the personal data into a registration screen, part of the process of website account creation. A member can then alter all but one item of this personal data his/her self by using a feature of the club website. A member cannot edit their e-mail address as this is the account name. Instead a member requests a change via the website

Principle	Requirement	Compliance Statement
		administrator who enacts the change. All changes to account details are audited. Data submitted on paper application forms cannot be changed, but this is unnecessary after membership has been granted.
5	Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	The personal data specified is required for the entire membership period of the person concerned. On leaving the club, or for other reasons such as failure to pay annual subscription, a member's details and account are deleted.
6	Personal data shall be processed in a manner that ensures appropriate technical and organisational security of those data, including protection against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage	Features provided in the technology supporting the club website offer industry standard countermeasures to prevent data loss or unauthorised access to data. All IT components are hosted by a specialist web hosting provider Netcetera, who host the website at a Tier 3 data centre and have ISO 27001 security certification. All communications between a member's client device (computer, phone, tablet) uses Public Key encryption (https) to protect member's passwords and contact details. All logins and account changes are audited by the website directly with reports available in real-time to administrators.
7	Personal data shall be processed in accordance with the rights of data subjects under this Act.	Positive opt-in to the club privacy notice is implemented, as is the ability to withdraw consent. Members can access their personal data and modify it at any time on the website.
8	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data	The club has no organisational need to transfer data anywhere to other organisations (other than the declared data processors) either in the UK or abroad. The data is solely for access by club members and for

Principle	Requirement	Compliance Statement
	subjects in relation to the processing of personal data.	managing handicaps, a golf necessity.

8. Actions on PIA Outcomes

This PIA has been produced post implementation of club website and personal data collection. Most privacy solutions described in Section 6 are already implemented. However, a few remain, and this section provides a list of outstanding potential solutions that will act to reduce risk further to the club and its members.

This table was initially produced to record the recommended actions and subsequently additionally serves to record the Club committee's decision on resolving the issue.

Action	Target Date	Responsibility	Outcome
Create a procedure for the removal of personal details when a member leaves the club.	May 2018	Committee	Agreed by committee meeting on 12/3/2018.
Consider whether bulk display of member contact details is acceptable. If not, instruct website management to alter function so that only individual member searches are possible.	May 2018	Committee	Agreed by committee meeting on 13/2/2018. The function was implemented on the website on 23/02/2018.
Consider whether wording regarding data protection on website registration form requires any amendment in the light of GDPR requirements on an individual's right to be informed about usage of their data.	May 2018	Committee	Agreed by committee. Wording aligned to GDPR requirements proposed and accepted. Implemented on website 14/02/2018.
Consider whether advice on password selection should be added to website	May 2018	Committee	As a golf club, it is agreed we should not be offering detailed security advice. Basic

Action	Target Date	Responsibility	Outcome
account registration form.			suggestions on password selection will be added to registration page.
Consider whether scope of this Impact Assessment should be widened to include paper records and data held on Handicap Master.	March 2018	Committee	Agreed by committee meeting on 13/2/2018. Version 0d of this document has been produced including this data.
Consider whether it is feasible to remove contact details if a member withdraws consent.	March 2018	Committee	Agreed at committee meeting on 12/3/2018. Club members who do not consent will have option of referring to club noticeboard for information.
Consider whether it is lower risk to secure junior's medical details further, resulting in longer access delays.	March 2018	Committee	Considered at committee meeting of 12/3/2018. Decision was to retain current method of holding Junior's details as fast access in an emergency is paramount.

9. Recommended Privacy Notice Wording

It is assessed that the club's most appropriate lawful basis for handling member's data is consent. In addition, legitimate interest applies to the registering of data with England Golf.

The recommended Privacy Notice to use is provided below and is designed to contain the information indicated by the GDPR:

- The name of our organisation
- The name of any third-party controllers who rely on consent
- Why we require the data
- What we do with the data
- Individuals can withdraw consent, the impact of this, and how they do it
- Includes a positive opt-in mechanism (non-defaulted tick-box).

PRIVACY NOTICE

- Your information will be used by Easthampstead Golf Club for the purpose of compiling a register of Members to contact you when required.
- Your phone number/email address will be included in the annual Members Handbook and be available on the Member's section of the club website to allow other Members to contact you to arrange matches etc.
- We may send you other information concerning Club events using your email address.
- Information including your name, date of birth and handicap will be registered with England Golf. Please read their privacy notice. Your competition results and handicap adjustments will be managed using software from HandicapMaster.
- Your data will be retained for as long as you remain a Member of the Club and will remain with England Golf unless you explicitly request removal.
- We do not make your information available to any other organisations.
- You may modify your own contact details at any time using the website or by contacting the Member Secretary.
- You may withdraw your consent at any time by contacting the Member Secretary and your contact details will be removed. This will obviously prevent Members of the Club being able to contact you in future.

☐ Please signify by ticking the box that you have read the above and agree to usage of your data as indicated.