CELTIC DOLPHINS SWIMMING CLUB

GENERAL DATA PROTECTION REGULATIONS

DATA PROTECTION POLICY

1.0 SUMMARY

1.1 This Policy has been devised by the Committee of the Celtic Dolphins Swimming Club ("the Committee"), to provide information regarding the application of the General Data Protection Regulations ("GDPR"), regarding the treatment of personal information ("personal data") held in relation to Club members and key personnel of the Celtic Dolphins Swimming Club ("the Swimming Club").

1.2 Swim Wales guidance has been used to inform the drafting of this Policy together with independent legal advice being sought as to its contents.

1.3 The Policy applies to all committee members, volunteers and any contractors or staff employed directly by the swimming club. It sets out our approach to the complex area of 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.

1.4 The Club Welfare Officer will be the designated ***Data Protection Officer*** ("DPO") and will oversee the implementation of this Policy in conjunction with the Committee and its Chair who is assigned the ***Data Controller***.

1.5. This information will also be available on the Swimming Club's website www.celticdolphinsswimmingclub.co.uk which will be used to direct enquiries to the DPO.

2.0 POLICY STATEMENT

2.1 The general aim of the GDPR is to ensure that where personal data is held it is held securely and the data is adequate, relevant and not excessive. GDPR also ensures that members of the Swimming Club and any Club personnel may request access and review of the contents of any files held on them in line with the provisions set out within GDPR.

2.2 Throughout a swimmers membership of the Swimming Club and for as long a period as is necessary following the termination of their membership, the Swimming Club will hold the personal data of that individual and any other data connected with that swimmer's membership of the Swimming Club . The Club will also stipulate how long it will keep this information for the purposes connected with a swimmers membership. The same approach will also apply regarding any personnel or contractors employed directly by the Club as well as those who support the Club in a volunteer capacity.

2.3 This Policy works in conjunction with the Club's other policies e.g. Disciplinary Policy and any other policies we implement from time to time.

2.4 The Swimming Club endorses and adheres to the data protection principles within the GDPR and

requires all employees, volunteers, committee members and contractors to similarly comply in relation to all personal data held by the Swimming Club.

2.5 Club personnel should at all times value the right to privacy of its members, staff and volunteers about whom information is held and manage their personal information professionally and to ensure it remains confidential and secure.

2.6 The aim of this document is to provide information relating to the Swimming Club's obligations in relation to data protection and offer guidance on how Club personnel are expected to handle personal data, receipt of a Subject Access Request ("SAR") and the treatment of a data breach under GDPR.

2.7 The misuse and unauthorised disclosure of personal data can lead to significant financial penalties and personal prosecution. As such any breaches of this Policy will be viewed very seriously. All Club personnel are expected to read this document carefully and make sure they are familiar with it.

2.8 Failure to comply with the Policy and the principles set out in the GDPR will result in swift action being taken by the Swimming Club in line with its Disciplinary Policy. In regards to the handling of data breaches, further details are set out in Paragraph 15.

3.0 SCOPE

3.1 This document applies to all Club personnel which includes the following:

- Employees
- Volunteers
- Committee Members
- Contractors

3.2 In terms of employees this Policy applies only to those who are employed directly by the Swimming Club. It does not include the employees of Celtic Leisure, who work in partnership with the Club to employ the majority of the Club's coaching team. Celtic Leisure employees are subject to that organisation's policies and procedures.

3.3 The principles in this document also apply to the following categories:

- Current and former Club members/ swimmer and their families
- Current and former employees of the Club
- Job applicants (successful and unsuccessful)
- Former job applicants (successful and unsuccessful)
- Volunteers at the Club (current and former)
- Current and former Committee Members of the Club
- Trainees / students undertaking training or placements activities at the Club (current and former)

4.0 WHAT IS PERSONAL DATA?

4.1 GDPR applies to any 'personal data' that is information about a living individual who is identified or who is identifiable by the data. Personal data may be (the list beneath is not exhaustive):

- Photographs
- Video/ CCTV footage

- Information held on a database
- Records

4.2 For example, these records may include (the list beneath is not exhaustive):

- Health records
- Training records
- Contact names and addresses
- Performance information on Club swimmers

4.3 Some personal data is also classed as 'sensitive' (now known as "special category data" under GDPR) and attracts a higher level of protection under the Regulations. For example, this includes information relating to race or ethnic origin, disability and gender identity.

5.0 PROCESSING DATA

5.1 The definition of processing data is very wide and encompasses almost everything from the collection and storage of data to its eventual destruction.

5.2 Where the Swimming Club processes data it must be done so fairly and lawfully; specifically (where it is the appropriate legal bases) consent must be received to process as well as to disclose the data where it is relevant to do so.

5.3 *Privacy Notice*

5.3.1 The following text will be applied as standard to any forms where personal data is requested by the Club.

GENERAL DATA PROTECTION REGULATIONS (GDPR)

The Celtic Dolphins Swimming Club is the data controller for the personal information you provide on this form. Your information will be used only for the purposes stated and will not be used for any other reason.

As the governing bodies for swimming in Wales and the UK, we may share your data with Swim Wales and British Swimming. We may also share details with Celtic Leisure as the membership body through which swimmers join the Club. We will not share your data with any other third parties without your explicit consent unless we are required or permitted to do so by law.

For further information about our Privacy Policy please visit www.celticdolphinsswimmingclub.co.uk

6.0 KEY PRINCIPLES

6.1 The Swimming Club will apply the following key data protection principles when processing data, that is, the data being collected will be:

- adequate, relevant and not excessive in relation to its purpose
- accurate and when necessary kept up to date
- not be kept for longer than is necessary
- be processed in accordance with the rights of the data subject under the Regulations
- be secured to protect against unauthorised or unlawful processing and accidental loss or destruction of or damage to personal data

7.0 CLUB OBLIGATIONS

7.1 The Swimming Club will ensure that all Club personnel work within the requirements of GDPR at all times to:

- Ensure that personal data is only disclosed to those who are entitled to receive it
- Take care to ensure that data stored both manually and on computer is secure, accurate and up to date

7.2 Club personnel MUST NOT:

- Disclose confidential information unless permission is granted by the data subject
- Use any personal data held by the Swimming Club for personal use

7.3 If there is any doubt about whether to disclose information, such matters should be referred to the DPO who will seek legal advice and/or escalate matters to the Committee if necessary.

8.0 INDIVIDUAL'S RIGHTS UNDER THE ACT

8.1 Section 3 sets out a list of individuals to whom this Policy applies. These individuals have the following rights:

- To ask the Club if it holds personal information about them
- To ask what it is used for
- To be given a copy of the information
- To be given details about the purposes for which the Club uses the information and of other organisations or persons to whom it is disclosed
- To ask for incorrect data to be corrected
- To be given an explanation as to how any automated decisions taken about them have been made
- To ask the Club not to use personal information for direct marketing, where its use is likely to cause unwarranted substantial damage or distress or lead to decisions which significantly affect the individual (based solely on the automatic processing of the data)

8.2 There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include (this list is not exhaustive) repeat access and/or vexatious requests, confidential references and third party information (for which consent is required).

8.3 If the Club receives a request for information from a third party (e.g. a legal advisor), we will take appropriate 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.

9.0 SUBJECT ACCESS REQUESTS

9.1 A request for a copy of information held about an individual is known as a Subject Access Request ("SAR").

9.2 All requests must be made in writing to the Club.

9.3 GDPR requires the Club to comply with SAR's within ***thirty days*** from receipt of the request.

10.0 WHAT IF THE DATA HELD IS INCORRECT?

10.1 If data is incorrect, the individual should write to the Club stating what data is incorrect and ask for the data to be corrected.

10.2 The Club must confirm with the individual what has been done within ***21 days*** of receiving the request.

11.0 WHAT IF THE APPLICANT IS NOT HAPPY WITH THE RESPONSE?

11.1 If an applicant considers their request has not been complied with, they have the right to request a review to Swim Wales setting out why they think that the information should have been provided to them.

11.2 If, following the investigation and review response from Swim Wales the individual remains dissatisfied with the outcome, they can complain to the regulator for privacy legislation which in this case is the Information Commissioner Office ("ICO") who, subject to their findings, has the ability to serve the Club with an information and/ or enforcement notice. Further information on about the ICO can be found at ico.org.uk.

11.3 Any such notices should be sent directly to the Club's DPO from the ICO. Similarly, in the event of a notice being served on the Club, the correspondent must immediately pass the communication to the DPO to address.

12.0 SUBJECT ACCESS REQUESTS - RESPONSE PROCEDURE

12.1 On receipt of a SAR, the Club's DPO will co-ordinate our response, which may include written material provided by external legal advisors if necessary. The action taken will depend upon the nature of the request.

12.2 The DPO will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/ email from the DPO should suffice in most cases.

12.3 The DPO will inform the Committee of any action that must be taken to legally comply. In conjunction with the Committee, the DPO will co-ordinate any additional activity to meet the request and will ensure that the relevant response is made within the time period required.

12.4 For more complex cases where further investigation and/ or legal advice is required, a 'holding' letter/ email will be sent to the applicant by the DPO advising of the situation and the anticipated timeframe.

13.0 SCHEDULE OF PERSONAL DATA PROCESSED BY THE CLUB

13.1 The Swimming Club will maintain a Schedule ("Schedule") of personnel data as processed by the Club.

13.2 The Schedule will set out the type of personal information that is typically held, for what purposes it is kept and over what timeframe as well as the measures that are in place to secure the data. In line with the Club's Privacy Notice above, details of any requirement to disclosure the data will also be included on the Schedule.

13.3. The Schedule will be monitored in accordance with the measures set out in Paragraph 14.0 below.

14.0 POLICY MONITORING

14.1 As the designated DPO, the Club's Welfare Officer will monitor the application of this Policy and will immediately report any data breaches and/ or breaches of the Policy to the Committee who will investigate and take the appropriate action. This process will be overseen by the Committee Chair in his/ her capacity as Data Controller.

14.2 The DPO will direct the Committee to review, and update where necessary, the Policy, Schedule of Personal Data and any other associated documentation on at least an annual basis.

14.3 The DPO will also communicate any changes in subsequent legislation to ensure that these are considered and the Policy is updated where relevant.

15.0 TREATMENT OF DATA BREACHES

15.1 Reporting a breach in the treatment of the data processed by the Club to the ICO is necessary only on occasion where there is a high risk to an individual, for instance if they are likely to suffer damage such as identity theft, financial loss, harm or discrimination.

15.2 *What is a breach?*

15.2.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

15.2.2 Personal data breaches can include (this is not an exhaustive list):

- access of a database by an unauthorised third party;
- sending personal data to the wrong recipient;
- devices such as USB sticks, laptops or mobiles containing personal data being lost or stolen; alteration of personal data without permission; and
- loss of availability (even if it is just temporary) of personal data, for example, where there has been a back-up failure.

15.3 *Notification Process*

15.3.1 When there is a *reasonable degree of certainty* that a data breach that affects personal data has occurred, the incident will be self-reported promptly to the ICO by the Club's Data Controller (i.e. the Committee Chair).

15.3.2 Where feasible, this will be no later than 72 hours after the Data Controller has become aware of the breach.

15.3.3 Communications regarding the breach will also be issued as soon as reasonably possible by the Committee to those affected by the incident.

16.0 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1 We will carry out a Data Protection Impact Assessment whenever the Club is planning to carry out a new *high risk* data processing activity. This will be directed by the DPO.

16.2 The DPIA will be used to help to determine the most effective way the Club can comply with the data protection legislation and help to identify any risks to the processing of the data and put measures in place to mitigate these risks.

16.2 Examples of when a DPIA might be required to be undertaken include the following (this is not an exhaustive list):

- when the Club engages in an information sharing operation with another organisation(s) (e.g. regional, local and national governing bodies) for a common purpose;

- when safeguarding information is to be shared;
- when there is a large scale or routine set of data being shared for a common purpose e.g. results from competitions.
- when a club is considering undertaking or engaging a new form of technology which will hold individuals' data

17.0 CLUB PERSONNEL - YOUR MAIN OBLIGATIONS

17.1 The main points of this Policy as it relates to the Club personnel involved in the operation and development of the Club is summarised as follows:

17.1.1 Treat all personal data with respect;

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

17.1.3 Immediately notify the Club's DPO (Welfare Officer) 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;

17.1.4 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

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

18.0 PRACTICAL MATTERS – DOS AND DON'TS

18.1 Whilst a common sense approach should be taken to the use and safeguarding of personal data and that all personal data should be treated with the upmost care and respect, set out below are some examples of the basic dos and don'ts which should be observed by all Club personnel:

18.1.1 Do not take personal data out of the pool premises (unless absolutely necessary).

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

18.1.3 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.

18.1.4 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.

18.1.5 If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

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

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

18.1.8 Do password protect documents and databases containing personal data.

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

18.1.10 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.

18.1.11 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.

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

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

18.1.14 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

18.1.15 Do challenge unexpected visitors accessing personal data.

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

18.1.17 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.

18.1.18 If taking down details or instructions from a member 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.

18.1.19 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.

18.1.20 Do not transfer personal data to any third party without prior written consent of the Club Committee via the DPO first.

18.1.21 Do notify the DPO immediately of any suspected security breaches or loss of personal data.

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

19.0 QUERIES

18.1 If you have any queries about this Policy please contact the designated DPO, the contact details of whom are available on the Club Notice Board at Pontardawe Pool or online at www.celticdolphinsswimmingclub.co.uk.