

Glenalbyn Swimming Club

GDPR Policy

July'2020

SWIM IRELAND
DATA PROTECTION
FOR CLUBS AND REGIONS
REVISED JUNE 2018

BACKGROUND

- i. During the course of your activities within your Club or Region you will collect, store and process the personal information of individuals. Under Irish law, this information must be treated in an appropriate and lawful manner.
- ii. The Data Protection laws in this area are the EU Regulation 2016/679 General Data Protection Regulation (“**GDPR**”) and other regulations. These Laws impose legal safeguards on how personal information which may be held on paper, computer or other media, may be treated.
- iii. Under the Laws, each Swim Ireland Club or Region is a ‘Data Controller’ of all personal data collected and used in that Club or Region. Swim Ireland clubs and regions are also data processors for Swim Ireland as they collect and provide Swim Ireland with membership, competition and squad information.
- iv. As a Data Controller you have a responsibility to establish practices and policies in line with the Laws. As Club/Regions are not required to appoint a Data Protection Officer to oversee compliance with data protection laws, Club/Regional Committees have overall responsibility for data protection compliance and implementation of this policy in your Club or Region. To contact Swim Ireland for further advice and or information please contact our Data Protection Compliance Committee at dataprotection@swimireland.ie.
- v. One of the main policies required under the Laws is a Data Protection Policy which sets out how personal data will be treated. Swim Ireland has put in place its own Policy and has prepared this Data Protection Policy Template that each Club/Region and Region can use in preparing its own Policy.
- vi. To prepare your own Data Protection Policy, please review below carefully and amend as you require. If you decide to use this template, this Background section should be deleted and the items in yellow square brackets below should be completed. You will see that some of the information in this background is duplicated below so that this background can be deleted without affecting your Policy.

Sarah Keane
Chief Executive Officer
Swim Ireland

Adam Cox
Membership Manager
Swim Ireland

July 2018

1. POLICY STATEMENT

- 1.1 Everyone has rights regarding how their personal information is handled. During the course of our activities Glenalbyn Swimming Club (“**we**”) will collect, store and process personal information and we recognise the need to treat it in an appropriate and lawful manner.
- 1.2 The types of information that we may be required to handle include details of current, past and prospective members, volunteers, contractors and others with whom we communicate.
- 1.3 The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the EU Regulation 2016/679 General Data Protection Regulation (“**GDPR**”) and other regulations. The Acts imposes restrictions on how we may use that information.
- 1.4 Under the Acts, we are known as the ‘Data Controller’ of all personal data used in our club. A Data Controller is the person who or organisation which determines the purposes for which, and the manner in which, any personal data is processed (“**Data Controller**”). As a Data Controller we have a responsibility to establish practices and policies in line with the Acts.
- 1.5 As we collect and pass data to Swim Ireland (“Data Controller”) we also act as a ‘Data Processor’ of personal data. We will only process personal data in accordance with instructions from the data controller.
- 1.6 We require each member, volunteer, contractor or other worker (“**you**”) to fully comply with this Policy. Any breach of this Policy will be taken seriously and may result in disciplinary action.
- 1.7 As Glenalbyn Swimming Club is not required to appoint a Data Protection Officer to oversee compliance with data protection laws, Glenalbyn Swimming Club Committee have overall responsibility for data protection compliance and implementation of this policy within Glenalbyn Swimming Club Any questions or concerns about the operation of this Policy should be referred in the first instance to swimmingclubglenalbyn@gmail.com
- 1.8 If you cannot answer the question internally the query can be referred to the Swim Ireland’s Data Data Protection Compliance Committee at dataprotection@swimireland.ie.
- 1.9 For further advice the Data Protection Commissioner can be contacted in the ROI at 1890 252 231 or 057 868 4800 and its website is www.dataprotection.ie. There is also a specific GDPR website which can be found at www.gdprandyou.ie. Within Northern Ireland further information can be found at <https://ico.org.uk>

2. STATUS OF THE POLICY

- 2.1 This Policy has been approved by Glenalbyn Swimming Club. It sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, storage, transportation and destruction of personal information.
- 2.2 If you consider that the Policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Committee of our Glenalbyn Swimming Club.

3. DEFINITION OF DATA PROTECTION TERMS

“Data” is information which is stored electronically, on a computer, or in structured paper-based filing systems.

“Data subjects” for the purpose of this Policy include all living individuals about whom we hold personal data. A data subject need not be an Irish national or resident. All data subjects have legal rights in relation to their personal data.

“Personal data” means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address, date of birth, image, sound recording or phone number) or it can be an opinion (such as the report of a competition).

“Data Controller” include employees or volunteers whose work involves deciding how personal data is used for. Data Controllers have a duty to protect the information they handle by following this Data Protection Policy at all times.

“Data Processors” include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf. Where we work with outside bodies or organisations and only process personal data on their behalf and under their instruction we may be the data processor of that organisation’s personal data.

“GDPR” The General Data Protection Regulation (GDPR) will replace current data protection laws in the European Union. The new law will give individuals greater control over their data by setting out additional and more clearly defined rights for individuals whose personal data is collected and processed by organisations.

“Processing” is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any action using the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

“Sensitive personal data” includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

4. DATA PROTECTION PRINCIPLES & MAIN OBLIGATIONS

4.1 The Data Protection laws set out six principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- (a) processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- (b) collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes (“purpose limitation”);
- (c) adequate and relevant, and limited to what is necessary to the purposes for which it is processed (“data minimisation”);
- (d) accurate and where necessary kept up to date;
- (e) kept for no longer than is necessary for the purpose (“storage limitation”);
- (f) processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures (“integrity and security”).

4.2 The main themes of the Data Protection laws are:

- (a) good practices for handling personal data;
- (b) rights for individuals in respect of personal data that data controllers hold on them; and
- (c) being able to demonstrate compliance with Data Protection laws.

4.3 In summary, the Data Protection laws require us to:

- (a) only process personal data for certain purposes;
- (b) process personal data in accordance with the 6 principles of ‘good information handling’ (including keeping personal data secure, processing it fairly and in a transparent manner and keeping it for no longer than is required);
- (c) provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice, for example you will have received one of these from us as a member of our club and one from Swim Ireland as a member of the organisation.
- (d) 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
- (e) keep adequate records of how data is processed and, where necessary, notify the regulator and possibly data subjects where there has been a data breach.

4.4 Your Main Obligations

- (a) Treat all personal data with respect;
- (b) Treat all personal data how you would want your own personal data to be treated;
- (c) Immediately notify your 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;
- (d) 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
- (e) Immediately notify our Committee if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this see our separate Data Breach Policy which applies to all members regardless of their position or role in Glenalbyn Swimming Club.

5. PRACTICAL GUIDANCE ON GDPR

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:

- (a) Do not take personal data out of the organisation's premises (unless absolutely necessary).
- (b) Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT support) and not to anyone else.
- (c) ONLY use specified club/region email addresses not personal email for undertaking club or region business
- (d) 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.
- (e) 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.
- (f) 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.
- (g) Where possible club/regions should purchase laptops for the sole use of club/region business and DO encrypt laptops, mobile devices and removable storage devices containing personal data.
- (h) Do password protect documents and databases containing personal data.
- (i) Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- (j) Use confidential waste disposal for any papers containing personal data or have them shredded before placing them in the ordinary waste disposal.
- (k) When in a 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.
- (l) Do not transfer personal data to any third party without prior consent or inline with your privacy policy
- (m) If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the Club Committee and Swim Ireland. For more details on this see our separate Data Breach Policy which applies to all members regardless of their position or role within the club.
- (n) If using messaging services i.e. WhatsApp, ensure that all members sign up to or opt into be contacted through this way and provide a means to opt out
- (o) Review membership/entry forms and adopt Swim Ireland templates where applicable

6. LAWFUL, FAIR AND TRANSPARENT PROCESSING

- 6.1 For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for our legitimate interest. Where an individual fills out a membership application form, enters a competition or joins a squad then it is understood that they consent to us having this information to process their membership or entry. However, if we wanted to use that membership data for another purpose, for example, to pass it to a third party, we will ask the individual for consent to this.
- 6.2 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
- a) The data subject has given consent to the processing of their personal data for one or more specific purposes. In respect of our club the processing is required for application of membership.
 - b) The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them
 - c) The processing is necessary for compliance with a legal obligation to which the data controller is subject
 - d) The processing is necessary to protect the vital interests of the data subject or of another natural person
 - e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or
 - f) The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- 6.3 When sensitive personal data is being processed (e.g. medical records of athletes), the data subject's explicit consent to the processing of such data will be required. Swim Ireland has amended its medical consent form to add in a Data Protection section and also declarations on Data Protection for the individual. An individual must declare he or she read and understood Glenalbyn Swimming Club privacy Policy and consents to Processing his or her sensitive personal data information. See Club/Region Privacy Policy on website for more information.
- 6.4 Where an outside organisation seeks to transfer personal data or sensitive personal data from its members, customers or suppliers to us, we must first ask that outside organisation to ensure that it is entitled to transfer that data to us and, where relevant, that it has obtained the consent from the relevant data subjects to the transfer to us. If an outside organisation proposes to transfer third party personal data to us and you are unsure whether you should accept such information, please contact our Committee for assistance.
- 6.5 If an outside organisation that you need to transfer personal data to is based outside the EEA, then special considerations may apply. This includes informing the data subject and asking for his or her consent to the transfer. Glenalbyn Swimming Club has included a section in its privacy Policy that informs individuals that their data may be transferred outside the EEA for processing and that the individual consents to this transfer. Where you think a transfer outside the EEA may take place and are concerned about the transfer, please contact our Committee

7. KEPT AND PROCESSED FOR SPECIFIED AND LAWFUL PURPOSES

- 7.1 Personal data may only be kept and processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR. This means that personal data must not be collected for one purpose and then used for another (e.g. videos taken of members competing at a swimming competition for training purposes and then used in a marketing campaign). If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose and written consent must be sought before any processing occurs.
- 7.2 Sensitive personal data such as medical records must be restricted to those who specifically need to access it. Physical records should be stored in locked filing cabinets. Electronic records should be encrypted with a password that is only known to those who need to access it. Those who do not need to access sensitive personal data are prohibited from accessing it.
- 7.3 Glenalbyn Swimming Club will complete an Club Processing Activities Log, this is a key step towards compliance with the GDPR's accountability principle, which requires us to demonstrate (and, in most cases, document) the ways in which we comply with data protection principles when transacting business.

8. DATA SECURITY

- 8.1 Glenalbyn Swimming Club shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 8.2 GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection through to the effective and safe destruction of that personal data. Personal data may only be transferred to a third-party organisation if it agrees to comply with those procedures and policies or puts in place its own adequate security measures.
- 8.3 Maintaining data security also means ensuring that the personal data is kept confidential. Only people who are authorised to access or use personal data should have access to it. This can be achieved by storing physical data in a filing cabinet or room that can be locked and the key is kept securely by one authorised person who can monitor access. On a computer security can be achieved by using document passwords and limiting access to shared folders.
- 8.4 Data Security storage and disposal procedures include:
- a) All electronic copies of personal data should be stored securely using passwords and data encryption
 - b) All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
 - c) It is best practice that personal data should not be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the club or otherwise without the approval of the committee and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary
 - d) No personal data should be transferred to any device personally belonging to a volunteer/member and personal data may only be transferred to devices belonging to the club/region, coaches, or other parties working on behalf of the Club/Region where the party in question has agreed to comply fully with this Policy and of the GDPR (which may include demonstrating to the Club/Region that all suitable technical and organisational measures have been taken)
 - e) Create specified email contacts for completing club/regional business
 - f) Paper documents should be shredded. Hard disc storage devices and other electronic storage devices should be physically destroyed when they are no longer required.
 - g) When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

9. ACCURATE DATA

- 9.1 Glenalbyn Swimming Club shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject,
- 9.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
- 9.3 Data subjects have the right to require Glenalbyn Swimming Club to rectify any of their personal data that is inaccurate or incomplete. Glenalbyn Swimming Club shall rectify the personal data in question, and inform the data subject of that rectification, within 30 days of the data subject informing Glenalbyn Swimming Club of the issue.

10. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

- 10.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. For example, where we do not need to know the religious beliefs of an individual to register them as a member, this will not be asked on membership application forms.

11. DATA RETENTION

- 11.1 Personal data will not be kept longer than is necessary for the reason it was collected. This means that data will be destroyed or erased from our systems when it is no longer required. For example, when a person does not renew his or her membership with us then we will not keep prior information collected on him or her indefinitely and we will delete it in line with our retention periods in appendix 1.
- 11.2 The Swim Ireland head office has a detailed Data Retention Policy in place. Where you have questions on how long you should retain certain data for that is not covered in the table below, you can request to see this Data Retention Policy or request the relevant maximum data retention period under this Policy. Please see appendix 1 for recommended retention periods.

12. DATA SUBJECT RIGHTS

12.1 Under GDPR Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

- (a) The rights to access their personal data, usually referred to as a subject access request
- (b) The right to have their personal data rectified;
- (c) The right to have their personal data erased, usually referred to as the right to be forgotten;
- (d) The right to restrict processing of their personal data;
- (e) The right to object to receiving direct marketing materials;
- (f) The right to portability of their personal data;
- (g) The right to object to processing of their personal data; and
- (h) The right to not be subject to a decision made solely by automated data processing.

12.2 The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by the committee of Glenalbyn Swimming Club without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay. Where a club/region has received a request in line with these rights, then the club/region will notify Swim Ireland (dataprotection@swimireland.ie) of this request

12.3 Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

12.4 If we receive the request from a third party (e.g. a legal advisor), we must take 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.

13. DEALING WITH DATA ACCESS REQUESTS

13.1 Data subjects may make Subject Access Requests ("SARs") at any time to find out more about the personal data which the Glenalbyn Swimming Club holds about them, what it is doing with that personal data and why.

13.2 Data subjects wishing to make a SAR may do so in writing, using the Club/Regions Subject Access Request Form (this can be found as Appendix 2), or other written communication. SARs should be addressed to the Glenalbyn Swimming Club Secretary. Swim Ireland will be notified of all requests at dataprotection@swimireland.ie.

13.3 Responses to SARs shall normally be made within 30 days of receipt, however, this may be extended by up to 60 days if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by Glenalbyn Swimming Club Committee.

- 13.5 Glenalbyn Swimming Club does not charge a fee for the handling of normal SARs. Glenalbyn Swimming Club reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. DATA BREACH NOTIFICATION

- 14.1 A **“Personal data breach”** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate actions.
- 14.2 Examples of a personal data breach include the following:
- a) Access by an unauthorised third party
 - b) Deliberate or accidental action (or in-action) by Club/Region or processor
 - c) Sending personal data to an incorrect recipient
 - d) Computing devices containing personal data being lost or stolen.
 - e) Alteration of personal data without permission
 - f) Loss of availability of personal data, e.g.
 - g) Where personal data has been deleted accidentally or maliciously
 - h) Where for example an encryption key has been lost.
- 14.3 All personal data breaches must be reported immediately to Glenalbyn Swimming Club Committee and Swim Ireland dataprotection@swimireland.ie.
- 14.4 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Commissioner’s Office is informed (breaches@dataprotection.ie) without delay, and in any event, within 72 hours after having become aware of it. Swim Ireland and the Club/Region will decide who will notify/report breach to the Data Commissioner’s office in line with the data breach policy.
- 14.5 If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, all affected data subjects are informed of the breach directly and without undue delay. Swim Ireland and the Club/Region will decide who will notify/report breach to the subject in line with the data breach policy.
- 14.6 Data breach notifications shall include the following information:
- (a) a description of the nature of the breach
 - (b) the name and contact details of the data protection officer or other contact point
 - (c) a description of the likely consequences of the breach
 - (d) a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 14.7 The club/region has a detailed data breach policy which outlines the process in more detail.

15. PROVIDING INFORMATION OVER THE TELEPHONE

- 15.1 We will not provide personal data over the phone unless we are sure you have the right to receive. Where you are asked to provide personal data, we should:
- (a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.
 - (b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
 - (c) Refer to Glenalbyn Swimming Club committee for assistance in difficult situations. No-one should be pressurised into disclosing personal information.

16. MONITORING AND REVIEW OF THE POLICY

- 16.1 This Policy should be reviewed periodically to ensure it is achieving its stated objectives. Swim Ireland will review its own Data Protection Policy and will issue and recommendations or updates that may be of assistance.
- 16.2 This Policy was adopted on 29th May 2020.

APPENDIX 1

TYPE OF INFORMATION	MAXIMUM RETENTION PERIOD	HOW TO DESTROY/ARCHIVE
Member data including contact details, emails and correspondences	12 months from member's departure from Club/Region	<ul style="list-style-type: none"> • Archive in a secure location • Delete from lists within 12 months of cancellation of membership (unless member requests immediate removal) • Shred physical files and delete from IT systems, address books, mobile phones 12 months
Member images and video footage	This data should be deleted as soon as it is not required but see 'How to Destroy/Archive' column for more detail.	<ul style="list-style-type: none"> • Our privacy Policy informs members that images, or video footage may be taken at training, events or competitions. • If a member objects or ask you to delete footage or an image this must be carried out immediately • Destroy the video once it is no longer required or within 6 months of a member leaving the Club/Region/Swim Ireland • If you would like to retain the image or video for longer than 6 months, the written permission of the member featured in that video or image must be sought. This permission must be retained to prove that you have the right to hold this video. If the video or image is destroyed at a future date, this written permission should be kept for a further 2 years past this date and then it can be destroyed
Member Medical Records	On departure	<ul style="list-style-type: none"> • Shred physical files and delete from IT systems on departure
Credit or debit card details	1 day where no valid reason for holding this data. Where a reason exists, the maximum retention period is 12 months	<ul style="list-style-type: none"> • Shred physical records and delete from IT systems immediately after processing unless there is a valid reason for holding • If retained on foot of a valid reason, shred physical files and delete from IT systems within 12 months
Bank account details	2 months from date when individual is no longer engaged with Club/Region	<ul style="list-style-type: none"> • Treasurer to delete it from his or her own records (unless you have a valid reason for holding it) • Treasurer to shred physical files and delete from IT

		systems within 2 months
Complaints or Disciplinary Matters	12 months from member's departure from Club/Region or whilst any sanction is active	<ul style="list-style-type: none"> Shred physical records and delete from IT systems after 12 months
Garda Vetting Information	DO NOT RETAIN	<ul style="list-style-type: none"> Transfer to National Children's Officer at Swim Ireland Head Office
Documents relevant to current or potential litigation, investigations, inquiries	DO NOT DESTROY	<ul style="list-style-type: none"> Transfer this information to Club/Region Chair or Secretary Under Irish Law there is a positive obligation to preserve documents where litigation is anticipated or ongoing. These documents must be preserved and not destroyed

Appendix 2 – Sample Subject Access Request Form

In compliance with Article 15 of the General Data Protection Regulation, [Club/Region] can use the following sample form for subject access requests however it is not mandatory to do so.

Sample Subject Access Request Form: Request for a copy of Personal Data

Important: a photocopy of your proof of identity (e.g. passport or driver's licence) and a photocopy of proof of address (e.g. utility bill) must accompany this Access Request Form (see Note below).

Section A - please complete this section

Full Name:

Postal address:

*Telephone/e-mail:

(include area code)

*As we may need to contact you to discuss your Access Request

Section B - please complete this section

I, [insert name] wish to have access to data that I believe [Club/Region] retains on me as outlined below (please include the name of service(s) and anything relevant to your access request)

Signed.....Date.....

Please return this form to the club/regional secretary at swimmingclubglenalbyn@gmail.com

Note: we require proof of the applicant's identity and address to ensure that the person making this access request is acting legitimately