ULVERSTON AMATEUR SWIMMING CLUB

Data Protection Policy

The Policy

Ulverston Amateur Swimming Club (**UASC, the Club**) is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our staff, volunteers and members,

This Data Protection Policy ("**Policy**") sets out the approach to data protection law and the principles that will apply to the processing of personal data. The aim of this Policy is to ensure that personal data is processed in accordance with the law and with the utmost care and respect.

This Policy applies to all Members in the Club. References in this Policy to "us", "we", "ourselves" and "our" are to Ulverston Amateur Swimming Club (UASC). References to "you", "yourself" and "your" are to each Member to whom this Policy applies.

UASC recognises that the members have an important role to play in achieving these aims. It is the responsibility of the members, therefore, to familiarise themselves with this Policy and to apply and implement its requirements when processing any personal data.

Data protection law is a complex area. This Policy has been designed to ensure that UASC is aware of the legal requirements imposed on it and on its members and to give practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law or of the responsibilities of UASC and its members in relation to data protection.

If at any time a member has any queries on this Policy, on the responsibilities of UASC or on any aspect of data protection law, then seek advice. Contact the secretary: secretary@uasc.me.uk.

This Policy is divided into two parts. Part 1 is to be read by all Members. Part 2 is to be read by all Members who work in the following fields: Committee Members; finance; data inputting, membership, information technology, coaching/teaching, Welfare and any other roles which involve the handling of personal data relating to individuals.

PART 1 – To be read by all Members

1. Who is responsible for data protection?

1.1 All members are responsible for data protection, and each person has their role to play to make sure that UASC is compliant with the data protection laws.

1.2 UASC is not required to appoint a Data Protection officer, and have chosen not to do so. However we have still appointed the Secretary to be responsible for overseeing our compliance with data protection laws and they can be reached at secretary@uasc.me.uk.

2. Why do we have a data protection policy?

2.1 It is recognised that the processing of an individuals' personal data in a careful and respectful manner cultivates a trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable the organisation to work more effectively with and to provide a better service to those individuals.

2.2 This Policy works in conjunction with other policies implemented by the Club from time to time.

3. **Status of this Policy and the implications of breach.**

3.1 Any breaches of this Policy will be viewed very seriously. All Members must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under the Disciplinary Procedure.

3.2 If Members do not comply with data protection laws and/or this Policy, then members are encouraged to report this fact immediately to the Chairman (chair@uasc.me.uk). This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date this Policy coming into force.

3.3 Also if a member is aware of or believe that any other member or representative of UASC is not complying with data protection laws and/or this Policy the member should report it in confidence to the Chairman (chair@uasc.me.uk). The Club's Whistleblowing Procedure will apply in these circumstances and the member may choose to report any non-compliance or breach through the confidential whistleblowing reporting facility.

4. **Other consequences**

4.1 There are a number of serious consequences for both the member and the Club if the Club does not comply with the data protection laws. These include:

4.1.1 For the member:

4.1.1.1 **Disciplinary action:** If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with the policies could lead to termination of your volunteering position..

4.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

4.1.1.3 **Investigations and interviews**: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

4.1.2 For the organisation:

4.1.2.1 **Criminal sanctions:** Non-compliance could involve a criminal offence.

4.1.2.2 **Civil Fines:** These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher. These amounts are very substantial.

4.1.2.3 **Assessments, investigations and enforcement action**: The Club could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

4.1.2.4 **Court orders:** These may require the Club to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

4.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of non-compliance by the Club.

4.1.2.6 **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become

public knowledge and might damage the brand. Court proceedings are public knowledge.

4.1.2.7 **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

5. Data protection laws

5.1 The Data Protection Act 1998 ("**DPA**") applied to any personal data that is processed by the Club and from 25th May 2018 this has been replaced by the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together "**data protection laws**") and then after Brexit the UK will adopt laws equivalent to these data protection laws.

5.2 This Policy is written with GDPR and the DPA 2018 both in force, i.e. it states the position as from 25th May 2018.

5.3 The data protection laws all require that the personal data is processed in accordance with the Data Protection Principles (see below) and gives individuals rights to access, correct and control how the organisation uses their personal data

6. Key words in relation to data protection

6.1 The following are key terms that are commonly used in relation to data protection:

6.1.1 **Personal data** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into the possession of the Club). That living individual might be an employee, member, coach, athlete, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

6.1.2 Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do if taken together with other information available to or obtainable by us (e.g. a job title and company name). More details on this can be found in part 2 of this Policy.

6.1.3 **Data subject** is the living individual to whom the relevant personal data relates.

6.1.4 **Processing** is widely defined under the data protection laws and generally any action taken by the Club in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

6.1.5 **Data controller** is the person who decides how personal data is used, for example the Club will always be a data controller in respect of personal data relating to our employees and members.

6.1.6 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

7. Outline

7.1 The main themes of the data protection laws are:

7.1.1 good practices for handling personal data;

7.1.2 rights for individuals in respect of personal data that data controllers hold on them; and

7.1.3 being able to demonstrate compliance with data protection laws.

7.2 In summary, the data protection laws require all members to:

7.2.1 only process personal data for certain purposes;

7.2.2 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);

7.2.3 provide certain information to those individuals about whom the Club process personal data which is usually provided in a privacy notice, for example every member will have received a copy as one of our members;

7.2.4 respect the rights of those individuals about whom the Club process personal data (including providing them with access to the personal data the Club hold on them); and

7.2.5 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.

7.3 Every Member has an important role to play in achieving these aims. It is the member's responsibility, therefore, to familiarise themselves with this Policy.

7.4 Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**") and they are the regulator for data protection in the UK. The ICO has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

8. Data protection principles

8.1 The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

8.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

8.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("**purpose limitation**");

8.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("**data minimisation**");

8.1.4 accurate and where necessary kept up to date;

8.1.5 kept for no longer than is necessary for the purpose ("**storage limitation**");

8.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

8.2 More details on these principles can be found in Part 2 of this Policy.

9. Data subject rights

9.1 Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

9.1.1 The rights to access their personal data, usually referred to as a subject access request;

9.1.2 The right to have their personal data rectified;

9.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

9.1.4 The right to restrict processing of their personal data;

9.1.5 The right to object to receiving direct marketing materials;

9.1.6 The right to portability of their personal data;

9.1.7 The right to object to processing of their personal data; and

9.1.8 The right to not be subject to a decision made solely by automated data processing.

9.2 Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances. More details on these rights can be found in Part 2 of this Policy.

10. **Member's main obligations**

10.1 What this all means for the member can be summarised as follows:

10.1.1 Treat all personal data with respect;

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

10.1.3 Immediately notify the Chairman, chair@uasc.me.uk 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;

10.1.4 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

10.1.5 Immediately notify the Chairman, chair@uasc.me.uk 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 the Club].

10.2 More detail on the obligations that apply to those staff who process personal data on behalf of the Club can be found in Part 2 of this Policy which will apply to any person who is in a position or role which involves the processing of personal data on behalf of the organisation.

11. **Members activities**

11.1 Data protection laws have different implications in different areas of the organisation and for different types of activity, and sometimes these effects can be unexpected.

11.2 Areas and activities particularly affected by data protection laws include Human Resources, membership. payroll, security (e.g. CCTV), member support, data inputting, marketing and promotions, health and safety, finance, performance and participation.

11.3 The Club must consider what personal data it might handle. It must consider carefully what the data protection laws might mean for it and its activities, and ensure that it complies at all times with this policy.

12. **Practical matters**

12.1 Whilst the Club should always apply a common sense approach to how it uses and safeguards personal data, and treats personal data with care and respect, set out below are some examples of dos and don'ts:

12.1.1 Do not take personal data out of the Club's premises (unless absolutely necessary).

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

12.1.3 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.

12.1.4 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.

12.1.5 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.

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

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

12.1.8 Do password protect documents and databases containing personal data.

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

12.1.10 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.

12.1.11 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., and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

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

12.1.13 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.

12.1.14 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.

12.1.15 Do challenge unexpected visitors or employees accessing personal data.

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

12.1.17 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.

12.1.18 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.

12.1.19 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.

12.1.20 Do not transfer personal data to any third party without prior written consent of [Insert the title of the person responsible

12.1.21 Do notify the Chairman mmediately of any suspected security breaches or loss of personal data.

12.1.22 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the Chairman. For more details on this see our separate Data Breach Policy which applies to all workers regardless of their position or role in our organisation.

12.2 However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of the Secretary.

13. **Queries**

13.1 If you have any queries about this Policy please contact the Secretary (secretary@uasc.me.uk).

13.2 There is also more detail on Data Protection contained in Part 2 of this Policy. Even if you are not required to read Part 2 of this Policy, you may find the answer to any queries you have in Part 2 and you are also encouraged to read Part 2.

PART 2 – To be read by all Members who work/volunteer in the following fields: Officers, Committee, Finance, Membership, Event Management, Data inputting, Information Technology, Coaching/Teaching and any other roles which involve the handling of personal data relating to individuals

Personal data

13.3 To expand on the information in Part 1 of this Policy data will relate to an individual and therefore be their personal data if it:

13.3.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

13.3.2 its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;

13.3.3 relates to property of the individual, for example their home, their car or other possessions;

13.3.4 it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);

13.3.5 is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;

13.3.6 has the individual as its focus, that is the information relates to the individual personally rather than to some other person or a transaction or event he was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;

13.3.7 affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;

13.3.8 is an expression of opinion about the individual e.g. records stored in the course of a coaching assessment or details regarding a participant's performance; or

13.3.9 is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

13.4 Information about Clubs or other legal persons who are not living individuals is not personal data. However, information about officers and volunteers, is often personal data, so business related information can often be personal data.

13.5 Examples of information likely to constitute personal data:

13.5.1 Unique names;

13.5.2 Names together with email addresses or other contact details;

13.5.3 Job title and employer (if there is only one person in the position);

13.5.4 Video - and photographic images;

13.5.5 Information about individuals obtained as a result of Safeguarding checks;

13.5.6 Medical and disability information;

13.5.7 Member profile information (e.g. marketing preferences); and

13.5.8 Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

13.6 Examples of information unlikely to constitute personal data:

13.6.1 Reference to the individual's name in a document that contains no other personal data about that them (e.g. including the individual in a list of attendees of a meeting where the individual attended in an official capacity on behalf of a company); and

13.6.2 Where the individual's name appears in an email that has been sent to or copied to them, but where the content is not about him or her (e.g. emails sent to the individual about an organisation's dealings).

14. Lawful basis for processing

14.1 For personal data to be processed lawfully, the organisation must process it on one of the legal grounds set out in the data protection laws.

14.2 For the processing of ordinary personal data in the organisation these may include, among other things:

14.2.1 the data subject has given their consent to the processing;

14.2.2 the processing is necessary for the performance of a contract with the data subject;

14.2.3 the processing is necessary for the compliance with at legal obligation to which the data controller is subject; or

14.2.4 the processing is necessary for legitimate interest reasons of the data controller or a third party i.e. you are processing someone's personal data in ways they would reasonably expect it to be processed and which have a minimal privacy impact on the data subject or where there is a compelling justification for the processing.

15. Special category data

15.1 Special category data under the data protection laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

15.2 Under data protection laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

15.3 To lawfully process special categories of personal data the organisation must ensure that one of the following conditions has been met:

15.3.1 the individual has given their explicit consent to the processing;

15.3.2 the processing is necessary for the performance of our obligations under employment law;

15.3.3 the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;

15.3.4 the processing relates to information manifestly made public by the data subject;

15.3.5 the processing is necessary for the purpose of establishing exercising or defending legal claims; or

15.3.6 the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

15.4 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and it is necessary to

15.4.1 ensure that either the individual has given their explicit consent to the processing; or

15.4.2 ensure that the processing of those criminal records history is necessary under a legal requirement imposed upon the organisation.

15.5 Normally special category personal data or criminal records history data would be processed in a Human Resources context and in the context of the members and volunteers etc. for [the purposes of health and safety requirements, safeguarding checks, etc.

16. **When does the Club process personal data?**

16.1 Virtually anything that is done with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. Storage of personal data is a form of processing. Process personal data bay be done using computers or manually by keeping paper records.

16.2 Examples of processing personal data might include:

16.2.1 Using personal data to correspond with members;

16.2.2 Holding personal data in our databases or documents; and

16.2.3 Recording personal data in personnel or member files.

17. **What does this mean?**

17.1 Personal data may be processed every day for any number of purposes and in any number of ways. Therefore it is necessary comply at all times with the Data Protection Principles.

18. **Data protection principles and what you must do**

18.1 There are 6 data protection principles. These principles must be complied with when process personal data.

18.2 There are indications in relation to each principle as to what must and must not be done. However, these are not exhaustive and for guidance only. It is necessary to use common sense and be mindful of the potential implications to an individual of the organisation processing their personal data. The principles are that personal data must be:

18.2.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

18.2.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("**purpose limitation**");

18.2.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("**data minimisation**");

18.2.4 accurate and where necessary kept up to date;

18.2.5 kept for no longer than is necessary for the purpose ("**storage limitation**"); and

18.2.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("**integrity and security**").

19. **Personal data must be processed fairly, lawfully and transparently.**

19.1 Personal data obtained illegally (e.g. stolen) must not be processed. Personal data must not be processed if obtained by misleading, pressurising or inducing an individual.

19.2 It is necessary to inform an individual: who the data controller is, the purpose for which personal data is to be processed; and any additional information that is necessary to ensure that the processing is fair and transparent.

19.2.1 In the majority of cases, it will be sufficient for the individual to have been provided with the privacy notice applicable to the category of individual to satisfy this requirement. This can be done by using the approved standard forms, contracts and terms, and approved scripts, that contain the relevant privacy notices. Therefore, it is necessary to use approved standard documents and scripts at all times.

19.2.2 If personal data is being processed in a new or extraordinary way, it is necessary to confirm that this is covered by our privacy notice. If in doubt, seek advice from the

20. **Personal data must be collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation").**

20.1 Personal data must be processed only for purpose for which it was collected e.g. if a member's details have been to forward information to them on the products and services available, the details must not be passed on to a third party seeking to promote their services.

20.2 If personal data is to be processed for another purpose, the individual must be informed of that purpose.

20.3 Again the purposes for which personal data is collect and process are set out in the standard privacy notices. This is another reason to make sure the standard documents are always used.

21. **Personal data must be adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation")**

21.1 It is necessary to ensure that the personal data collected can be used for the purposes for which it was collected. This means collecting what is needed to be collected, but not more personal data than is needed nor too little personal data.

21.2 If insufficient personal data is collected to utilise it for its intended purpose, it should be securely deleted or destroyed.

21.3 If more personal data than is required has been collected, the unnecessary personal data should be securely deleted or destroyed.

21.4 When collecting personal data or recording personal data, think whether it is in fact needed for the purpose for which it is collected.

22. **Personal data must be accurate and, where necessary, kept up to date.**

22.1 When recording personal data make sure that it is recorded accurately. This is always important, but especially so where personal data is being entered into a database that may be reused on numerous occasions. Any mistakes or errors in the personal data will repeat themselves each time it is used.

22.2 Wherever possible, it is necessary to regularly confirm that personal data is correct and update databases accordingly (noting if personal data is incorrect and correcting it accordingly).

22.3 Where you become aware that personal data is incorrect, then the personal data should be corrected to remove the errors.

23. **Personal data must be kept for no longer than is necessary for the purpose ("storage limitation").**

23.1 Data must be deleted when it is no longer required to fulfil the purposes for which it was originally collected.

23.2 Retention periods for data will be as set out in the standard privacy notice provided to the individual.

23.3 What is 'necessary' will depend on the circumstances. Common sense must be used and if in doubt, seek advice. Once deleted it may not be possible to retrieve personal data deleted in error so it is always best to check before permanently deleting any personal data.

24. **Personal data must be processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security")**

24.1 What are appropriate measures will depend on the circumstances, particularly the nature of the personal data that is being processed, the harm that might result to the individual, the technologies available to keep personal data secure (e.g. encryption software) and the cost of measures.

24.2 Most of the technical and organisational measures are set by the organisation, and it is just necessary to follow them. Therefore it is necessary to follow all security policies, guidelines and instructions that are issued at all times. This includes both security for electronic systems and devices and physical security.

24.3 Specific parts of the Club will have responsibility for implementing various technical and organisational measures to protect personal data, for example IT in relation to the computer systems, and HR in relation to any Members.

25. **Foreign transfers of personal data**

25.1 Personal data must not be transferred outside the European Economic Area (**EEA**) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or adequate protections are put in place.

25.2 These protections may come from special contracts that need to be put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection.

25.3 These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of the affiliated organisations.

25.4 Under no circumstances must the transfer of any personal data outside of the EEA take place without Secretary's prior written consent.

25.5 It will also be necessary to inform data subjects of any transfer of their personal data outside of the UK and may be necessary to amend their privacy notice to take account of the transfer of data outside of the EEA.

25.6 For any person involved in any new processing of personal data which may involve transfer of personal data outside of the EEA, then please seek approval of the Secretary prior to implementing any processing of personal data which may have this effect.

26. **Data subject rights**

26.1 Individuals have certain rights under data protection laws (**Rights**). These are:

26.1.1 the right of access (also known as a data subject access request)

26.1.2 the right to rectification

26.1.3 the right to erasure (also known as the right to be forgotten)

26.1.4 the right to restrict processing

26.1.5 the right to data portability

26.1.6 the right to object

26.1.7 rights in relation to automated decision making and profiling.

26.2 The exercise of these Rights may be made in writing, including email, and verbally and should be responded to in writing by the organisation (if the organisation is the relevant data controller) 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. The organisation must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

26.3 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.

26.4 If the request is received from a third party (e.g. a legal advisor), the organisation 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.

26.5 There are very specific exemptions or partial exemptions for some of these Rights and they will be discussed in relation to the specific right in sections 29 to 38 below.

26.6 Where an individual considers that the organisation has not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation.

26.7 The individual can also complain to the regulator for privacy legislation, which will usually be the ICO, and they can also make the Club comply and can also impose a civil fine.

26.8 In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the data protection laws. The ICO must investigate and may serve an information notice on the organisation (if the organisation is the relevant data controller) to obtain relevant information. The ICO may also conduct an informal investigation to start with, usually by writing a letter asking the organisation to explain the position.

26.9 The result of any investigation may lead to an enforcement notice being issued by the ICO. Any letters, assessments, information notices or enforcement notices from the ICO should be immediately sent directly to the Secretary.

27. **Notification and response procedure**

27.1 If a verbal request is received in relation to a Right, or believe a verbal request has been made for the exercise of a Right then:

27.1.1 pass the call or person to the Secretary if possible. The Secretary should make a written record of all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to the Secretary. If it is not possible to transfer the individual over then make a written record of the request and contact details for the individual making the request; and

27.1.2 inform the Chairman of the request and pass to them any written records relating to the request.

27.2 If a letter or fax exercising a Right is received then:

27.2.1 pass the letter to the Secretary.

27.2.2 the Secretary must log the receipt of the letter.

27.2.3 The Secretary will then respond to the individual on behalf of the organisation.

27.3 If an email exercising a Right is received by then:

27.3.1 pass the email to the Secretary;

27.3.2 the Secretary must log the receipt of the email

27.3.3 the Secretary will then respond to the individual on our behalf.

27.4 The Secretary will co-ordinate the response of the organisation which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request and the Right. The Secretary will write to the individual and explain the legal situation and whether the organisation will comply with the request. A standard letter/email from the Secretary should suffice in most cases.

27.5 The Secretary will inform the other Club Officers of any action that must be taken to legally comply with any exercise of rights. The Secretary will also co-ordinate any additional activity required by the Committee or individual Committee members to meet the exercise of any of the Rights.

27.6 The Secretary will be responsible for ensuring that the relevant response is made within the time period required.

28. **How to locate information for data subject right requests and requests for the right to be forgotten**

28.1 If a person is responsible for carrying out or co-ordinating any searches for personal data then this section will assist in how the search should be approached.

28.2 The personal data to be provided in response to a subject access request, right to be forgotten or any other exercise of data subject rights may be located in several filing and/or network systems, so it is important to identify at the outset the type of information requested to enable a focused search.

28.3 However it should be noted that the individual is not obliged to clarify the scope of the search, so whilst it is possible to ask a useful clarification to the request my not be received or any response at all. In this case the Club will still have to comply with the original request.

28.4 Depending on the type of information requested, it may be necessary to search all or some of the following:

28.4.1 electronic systems (e.g. databases, non-networked computers, workforce records system, email data);

28.4.2 manual/paper filing systems (but only if they are 'structured filing systems', on which see below); and

28.4.3 any data systems held externally by our data processors.

28.5 If a person is not authorised to access the relevant system or files that need to be searched, then that person will not be able to carry out the search in those systems or files. In this case the person will need to delegate those aspects of the search to a person who is authorised to access the relevant system or files.

28.6 A reasonable search of the content of the relevant systems using the individual's name, membership number, address, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different, and it will be necessary to check with the Secretary before commencing any search.

28.7 If information is not part of a structured filing system, it does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

28.8 To be a structured filing system, the system must be:

28.8.1 contain information relating in some way to individuals. Usually, there would be more than one file in the system or a group of information referenced by a common theme (e.g. an absence spread sheet). The files need not be located in the same geographical location, but could be dispersed over different locations;

28.8.2 structured by reference to individuals (e.g. by name or membership or account number) or by reference to information relating to individuals (e.g. type of role or address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held; and

28.8.3 structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced so as to easily indicate whether and where in the file data about the individual is located.

28.9 Therefore, a structured filing system which is subject to the data protection laws must have an external and internal structure which allows personal data about an individual to be located relatively easily without having to conduct a manual search of the entire file. If it is necessary to thumb through the whole file to find specific information, the file is not a structured filing system.

28.10 It might help to apply the 'temp test' to determine if a system is a relevant filing system. Ask yourself if a temp with no specialist knowledge of the internal processes and procedures could, if asked to retrieve information about a specified individual, identify that the system might hold such information and where in that system the information would be. If so it will be a structured filling system.

28.11 It will be necessary to liaise with the Secretary in relation to the searches to be carried out and they will also liaise with other committee members and volunteers to carry out searches of any physical files or records.

29. **Right of Access**

29.1 This paragraph contains the specific procedure to be followed where an individual exercises their right of access (also known as a data subject access request). The request need not refer to the Right, for instance, it might simply request 'a copy of all the information that Club has about the person.

29.2 There are limited timescales within which the Club must respond to a request and any delay could result in the Club failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

29.3 The data protection laws gives individuals the right to obtain:

29.3.1 confirmation that their personal data is being processed;

29.3.2 access to their personal data; and

29.3.3 access to other supplementary information.

29.4 The individual is entitled to receive a description of the following:

29.4.1 the purposes for which we process the data;

29.4.2 the categories of personal data that is process about them;

29.4.3 the recipients to whom the Club may disclose the data;

29.4.4 the duration for which the personal data may be stored;

29.4.5 the rights of the data subject under the data protection laws;

29.4.6 any information available regarding the source of the data were it is not collected from the data subject direct;

29.4.7 the right of the data subject to make a complaint to the supervisory authority for data protection;

29.4.8 the logic behind any automated decision the Club has taken about him or her (see below), the significance and consequences of this automated processing.

29.5 Plus the Club must also provide the information constituting the individual's personal data which is within the scope of their request. The Club must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically the Club can, unless the data subject specifies otherwise, also provide the information in electronic form.

29.6 If the individual requests details on automatic decisions made about him, the Club must provide appropriate information.

29.7 The Club may:

29.7.1 ask for additional information to confirm the identity of the individual making the request;

29.7.2 request that the scope of the request is narrowed in order to ease the searches to be undertaken (but the individual does not have to agree to such a request from the Club; and

29.7.3 where requests are manifestly unfounded or excessive, because they are repetitive: (a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or (b) or refuse to respond. Where the Club refuse to respond to a request, the Club must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

29.8 Where the Club process a large quantity of information about an individual, the data protection laws permit the Club to ask the individual to specify the information the request relates to. The legislation does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

29.9 The Club should verify the identity of the person making the request, using "reasonable means" if the Club is not sure about their identity.

30. **Redactions**

30.1 Where the Club is providing information to an individual where they have made a subject access request, they are only entitled to their personal data. They are not entitled to see information which relates to other individuals or to other Clubs,

30.2 In these cases the Club would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

31. **Disclosing personal data relating to other individuals**

31.1 Sometimes information that is determined to be personal data about one individual might include information identifying or personal data about another person (e.g. an email between two people might contain personal information relating to both the sender and the recipient) and in some cases it is not possible to redact the information about the other person. There are additional steps to consider in relation to whether the Club discloses this information.

31.2 The Club must consider whether the other person has consented to the disclosure of their information or whether it would be reasonable to comply with the request without the other person's consent.

31.3 Where the other person has consented, their information can be disclosed.

31.4 Where the other person has not consented, whether it would be reasonable to disclose that person's information will depend upon all the circumstances and these must assess on a case by case basis.

31.5 The Club would consider whether:

31.5.1 The other person has refused their consent;

31.5.2 The other person's consent cannot be obtained (e.g. because they are incapable of giving it due to illness or incapacity);

31.5.3 Asking for consent might reveal the identity of the individual making the request;

31.5.4 The Club owes the other person a duty of confidentiality;

31.5.5 The Club has taken steps to obtain the consent of the other person;

31.5.6 The other person is a recipient or one of a class of recipients who might act on the data to the individual's disadvantage;

31.5.7 The other person is the source of the information;

31.5.8 The information is generally known by the individual; and

31.5.9 The individual has a legitimate interest in the disclosure of the other person's information which they have made known to us.

31.6 If the Club decides that the other person's information should be withheld (usually it should be), the Club still has to provide as much of the information requested as

possible. Therefore, the Club should protect the other person's identity by redacting as much of this information and other identifiable particulars.

31.7 Always keep a record of what you have decided to do and your reasons for doing it.

32. Exemptions to the right of subject access

32.1 In certain circumstances the Club might be exempt from providing personal data in response to a subject access request. These exemptions are described below and should only be applied on a case by case basis after a careful consideration of all the facts.

32.2 Crime detection and prevention

32.2.1 The Club does not have to disclose personal data that we process for the purposes of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting any tax or duty, if and to the extent that giving subject access would be likely to prejudice any of these purposes.

32.3 Confidential references

32.3.1 The Club does not have to disclose certain confidential references that the Club has given to third parties, but might have to disclose confidential references that the Club receive from third parties. Bear in mind that references received from third parties may contain personal data of another person, so it is necessary to consider the rules regarding disclosure of other party's personal data set out above.

32.4 Legal professional privilege

32.4.1 The Club does not have to disclose any personal data that is legally privileged. The following would be legally privileged:

32.4.1.1 confidential communications between the Club and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice; and

32.4.1.2 confidential communications between the Club or our lawyers and a third party (e.g. a witness) where the dominant purpose of the communication is to give or seek legal advice in respect of current or potential legal proceedings. This claim to legal privilege would end as soon as the case has been decided and, at that moment, the documents in the file might be disclosable if a subject access request is received.

32.5 Management forecasting

32.5.1 The Club does not have to disclose any personal data which the Club process for the purposes of management forecasting or management planning to assist the Club in the conduct of any organisation or any other activity (e.g. succession planning, volunteer recruitment or reorganisation) if and to the extent that disclosing the personal data would be likely to prejudice the conduct of that organisation or activity.

32.6 Negotiations

32.6.1 The Club does not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

32.7 In any cases of doubt then speak to the Secretary and it may be that external legal advice is necessary in relation to whether or not an exemption can be applied in a particular case.

33. **Right to Erasure**

33.1 The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

33.2 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

33.2.1 where their personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

33.2.2 when the individual withdraws consent (but only to the extent that consent is the only basis for processing their personal data);

33.2.3 when the individual objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing;

33.2.4 where their personal data was unlawfully processed;

33.2.5 where their personal data has to be erased in order to comply with a legal obligation; and

33.2.6 where their personal data is processed in relation to the offer of information society services to a child.

33.3 There are some specific circumstances where the right to erasure does not apply and the Club can refuse to deal with a request:

33.3.1 to exercise the right of freedom of expression and information;

33.3.2 to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;

33.3.3 for public health purposes in the public interest;

33.3.4 archiving purposes in the public interest, scientific research historical research or statistical purposes; or

33.3.5 the exercise or defence of legal claims.

33.4 If the Club has disclosed the personal data to be erased to third parties, the Club must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

34. **Right to rectification**

34.1 An individual has the right to ask the Club to:

34.1.1 correct inaccurate personal data;

34.1.2 complete information if it is incomplete; and

34.1.3 delete personal data which is irrelevant or no longer required for our purposes.

34.2 If the Club has disclosed the personal data in question to third parties, the Club must inform them of the rectification request where possible. The Club must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

34.3 If data is factually correct and the Club is justified in keeping it, i.e. it is relevant to the lawful purpose the Club is holding it for then the Club does not have to change or delete it, but the individual may make a request for erasure, i.e. the right to be forgotten, and in that case the Club would have to analyse the personal data and whether it can be retained based on that Right.

34.4 Where the Club is not taking any action in response to a request for rectification, the Club must explain why to the individual, informing them of their right to complain to the supervisory authority (usually the ICO) and to seek a remedy from the Courts.

35. **Right to Restrict Processing**

35.1 An individual is entitled to require the Club to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. The Club can retain just enough information about the individual to ensure that the restriction is respected in future.

35.2 The Club will be required to restrict the processing of personal data in the following circumstances:

35.2.1 where an individual contests the accuracy of the personal data, the Club should restrict the processing until the Club has verified the accuracy of the personal data;

35.2.2 where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the Club is considering whether legitimate grounds of the Club override those of the individual;

35.2.3 when processing is unlawful and the individual opposes erasure and requests restriction instead; and

35.2.4 if the Club no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

35.3 Previously given consent for processing can be revoked at any time by the individual, therefore the Club cannot justify continued processing of data as a result of a previous consent.

35.4 The Club must inform individuals when the Club decides to lift a restriction on processing (for example, if an individual contested our right to process their personal data on legitimate interest grounds and the Club subsequently found that the processing was justified on these grounds).

35.5 If the Club has disclosed the restricted personal data to third parties, the Club must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

36. **The Right to Data Portability**

36.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, the Club may be required to transmit the data directly to another organisation if this is technically feasible. However, the Club is not required to adopt or maintain processing systems that are technically compatible with other organisations.

36.2 The right to data portability only applies:

36.2.1 to personal data an individual has provided to a data controller;

36.2.2 where the processing is based on the individual's consent or for the performance of a contract; and

36.2.3 when processing is carried out by automated means.

36.3 The Club must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data.

This enables other organisations to use the data. The information must be provided free of charge.

36.4 If the personal data concerns more than one individual, the Club must consider whether providing the information would prejudice the rights of any other individual.

37. **Right to Object**

37.1 Individuals have the right to object to:

37.1.1 processing based on legitimate interests;

37.1.2 the performance of a task in the public interest/exercise of official authority (including profiling);

37.1.3 direct marketing (including profiling); and

37.1.4 processing for purposes of scientific/historical research and statistics.

37.2 If the Club process personal data on the basis of a legitimate interests or the performance of a task in the public interest/exercise of official authority:

37.2.1 individuals must have an objection on "grounds relating to his or her particular situation"; and

37.2.2 the Club must stop processing the personal data unless the Club can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

37.3 If the Club process personal data for direct marketing purposes:

37.3.1 The Club must stop processing personal data for direct marketing purposes as soon as the Club receives an objection. There are no exemptions or grounds to refuse;

37.3.2 the Club must deal with an objection to processing for direct marketing at any time and free of charge; and

37.3.3 the Club must nevertheless comply with the terms of the Privacy and Electronic Communication Regulations and the e-Privacy Regulation which replaces it.

37.4 If the Club process personal data for research purposes:

37.4.1 individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes; and

37.4.2 If the Club is conducting research where the processing of personal data is necessary for the performance of a public interest task, the Club is not required to comply with an objection to the processing.

37.5 If the Club's processing activities fall into any of the above categories and are carried out online, the Club must offer a way for individuals to object online.

37.6 The Club must inform individuals of their right to object "at the point of first communication" and in the privacy notices. This right must be "explicitly brought to the attention of the data subject and is to be presented clearly and separately from any other information".

38. **Automated decision making and profiling**

38.1 The privacy legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

38.2 The Club does not currently undertake any automated decision making.

39. **Enforcement**

39.1 If an individual disagrees that the Club has properly complied with a Right or the Club fails to respond they may apply to a Court for an order or complain to the ICO in each case requiring us to properly perform the Right.

39.2 If the Court or the ICO agrees with the individual it can:

39.2.1 order the Club to properly carry out the Right and what steps are needed to do this; and

39.2.2 order the Club to notify third parties who we have passed the data onto of the Right;

39.3 A court can also award compensation to the individual for any damage they have suffered as a result of the non-compliance by the Club. The ICO can also impose a civil fine upon the Club. These fines can be very substantial.

40. **Deleting personal data in the normal course**

40.1 The Club is only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, the Club is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

40.2 What the Club cannot do is amend or delete data because the Club does not want to supply it or because of the exercise of a Right.

Revision 1 12th December 2018