Data Protection Policy

Our Policy

Keynsham Amateur Swimming Club (KASC) is committed to complying with data protection law and to respect the privacy rights of individuals. The policy applies to everybody who processes personal data for the purposes of running the organisation and includes employees, officers, officials, coaches, volunteers and consultants engaged by the organisation ("**Representatives**").

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

This Policy applies to all squads within KASC. References in this Policy to "us", "we" and "our" are to the club as a whole or to the governing committee. References to "you", "yourself" and "your" are to each Representative to whom this Policy applies.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data. ***Please pay special attention to sections 13, 14 and 15 as these set out the practical day to day actions that you must adhere to when working or volunteering for the club.***

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you 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 nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact the individual appointed by the club committee as the Information Governance Officer who is responsible for the club's data protection compliance.

1. Who is responsible for data protection?

1.1 All our Representatives are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2 We are not required to appoint a Data Protection Officer (DPO), however we have still appointed a member of the committee to be responsible for overseeing our compliance with data protection laws and they have the title of Information Governance Officer.

2. Why do we have a data protection policy?

2.1 We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our 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 us 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 Representatives must read this Policy carefully and make sure they are familiar with it.

3.2 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the Information Governance Officer. 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 you are aware of or believe that any other representative of ours is not complying with Data Protection Laws and/or this Policy you should report it in confidence to the Information Governance Officer.

4. **Other consequences**

4.1 There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

4.1.1 For you:

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 our policies could mean that it may no longer possible for you to volunteer with us.

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 €20 million.

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

4.1.2.4 **Court orders:** These may require us 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 our non-compliance.

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 our reputation. Court proceedings are public knowledge.

4.1.2.7 **Loss of business:** Prospective members, athletes, volunteers, coaches, sponsors, suppliers and contractors might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.

4.1.2.8 **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 Previously, the Data Protection Act 1998 ("**DPA**") applied to any personal data that we processed. From 25th May 2018 this was 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 The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

5.3 In addition to the Data Protection Laws, this policy also requires us at all times to comply with the Privacy and Electronic Communications Regulations 2003 when processing personal data.

6. Glossary of terms

6.1 **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 our possession). That living individual might be an employee, member, prospective member, athlete from another club, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. photograph).

6.2 **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. if a name or a Swim England ID number) or might do if taken together with other information available or obtainable to us (e.g. a position title such as Head Coach, and a club name).

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

6.4 **Processing** is widely defined under data protection law and generally any action taken by us 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 photographs and video.

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

6.6 **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. Personal data

7.1 Data will relate to an individual and therefore be their personal data if it:

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

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

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

7.1.4 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);

7.1.5 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;

7.1.6 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 she/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;

7.1.7 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;

7.1.8 is an expression of opinion about the individual; or

7.1.9 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).

7.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.

7.3 Examples of information likely to constitute personal data:

7.3.1 Unique names;

7.3.2 Names together with email addresses or other contact details;

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

7.3.4 Video - and photographic images;

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

7.3.6 Medical and disability information;

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

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

8. Lawful basis for processing

8.1 For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

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

8.2.1 the data subject has given their consent to the processing (perhaps on their membership application form)

8.2.2 the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);

8.2.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject (such as reporting employee PAYE deductions to the tax authorities); or

8.2.4 the processing is necessary for the legitimate interest reasons of the organisation or a third party such as a leisure centre operator (for example, keeping in touch with members, athletes, participants about competition dates, upcoming fixtures or access to club facilities).

8.3 We process the personal data of children and we recognise that there are additional steps we must take to acknowledge the fact that children are less aware of the risks involved. These additional steps will include:

8.3.1 When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us;

8.3.2 When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract;

8.3.3 When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing and put age appropriate safeguards in place;

8.3.4 We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand;

8.3.5 We tell children what rights they have over their personal data in language they can understand.

9. Special category data

9.1 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.

9.2 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.

9.3 To process special categories of personal data lawfully we must also ensure that either the individual has given their explicit consent to the processing, or that another of the following conditions has been met:

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

9.3.2 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 situations;

9.3.3 the processing relates to information manifestly made public by the data subject themselves (as opposed to being posted on social media by someone else);

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

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

9.4 To process personal data relating to criminal records and history lawfully there are even more limited reasons, and we must either:

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

9.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

9.5 We would normally expect to process special category personal data or criminal records history data usually in a Human Resources context however this may also occur in the context of our athletes, coaches and volunteers for monitoring performance, health and safety requirements, and for safeguarding checks.

9.6 **When do we process personal data?**

9.7 Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

9.8 Examples of processing personal data might include:

9.8.1 Using personal data to correspond with members;

9.8.2 Holding personal data in our databases or documents; and

9.8.3 Recording personal data in personnel or member files.

10. **Outline**

10.1 The main themes of the Data Protection Laws are:

10.1.1 good practices for handling personal data;

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

10.1.3 being able to demonstrate compliance with these laws.

10.2 In summary, data protection law requires us as a data controller to:

10.2.1 process personal data only for certain purposes;

10.2.2 process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);

10.2.3 be transparent and provide certain information to those individuals about whom we process personal data which is usually provided in the form of a privacy notice. You will have received one of these from us as one of our Representatives;

10.2.4 respect the rights of those individuals about whom we process personal data (including providing them with access to their personal data we hold); and

10.2.5 keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

10.3 Every Representative has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

10.4 Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

11. Data protection principles

11.1 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:

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

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

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

11.1.4 accurate and where necessary kept up to date;

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

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

12. Data subject rights

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

12.1.1 The right to access their personal data, usually referred to as a subject access request

12.1.2 The right to have their personal data rectified;

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

12.1.4 The right to restrict processing of their personal data;

12.1.5 The right to object to receiving direct marketing materials;

12.1.6 The right to portability of their personal data;

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

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

12.2 The exercise of these Rights should be made in writing, including email, and should be responded to in writing by us (if we are 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. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

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 We must not disclose any personal information without we are certain that the data subject is who they say they are.

12.5 Parents of children over the age 12 do not automatically have the right to see the personal information of their children; we require the consent of the child in these circumstances to disclose such information.

12.6 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.

12.7 There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right not to receive marketing material is an absolute right, so this should be complied with immediately.

12.8 Where an individual considers that we have 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. The data subject can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

12.9 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 privacy legislation. The ICO must investigate and may serve an “Information Notice” on us (if we are the relevant data controller). The result of the investigation may lead to an “Enforcement Notice” being issued by the ICO. Any such

assessments, information notices or enforcement notices should be sent directly to our Information Governance Officer from the ICO.

12.10 In the event of a Representative receiving such a notice, they must immediately pass the communication to our Information Governance Officer.

13. Your main obligations

13.1 What this all means for you can be summarised as follows:

13.1.1 Treat all personal data with respect;

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

13.1.3 Immediately notify your discipline secretary or the Information Governance Officer if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

13.1.4 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

13.1.5 Immediately notify the Information Governance Officer 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 our Representatives regardless of their position or role in our organisation.

14. Your activities

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

14.2 Areas and activities particularly affected by data protection law include membership, finance, coaching, competitions and health and safety.

14.3 You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

15. Practical matters

15.1 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:

15.1.1 Do not disclose your unique logins and passwords for any of our IT systems to anyone else.

15.1.2 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.

15.1.3 Never leave any items containing personal data in insecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

15.1.4 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.

15.1.5 **Always** encrypt laptops, mobile devices and removable storage devices containing personal data.

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

15.1.7 Do password protect documents and databases containing personal data.

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

15.1.9 When picking up printing from any shared printer always check to make sure you have collected all of the printed matter that you expect. If the printer has run out of paper it may print out your document containing personal information when a third party subsequently restocks the printer with paper.

15.1.10 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.

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

15.1.12 When in public place, e.g. pool gallery or leisure centre 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.

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

15.1.14 Do challenge anyone you see unexpectedly accessing files or personal computers.

15.1.15 Do not leave personal data lying around, store it securely. This includes any personal information taken on poolside.

15.1.16 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.

15.1.17 If taking down details or instructions from a customer 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.

15.1.18 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.

15.1.19 Never disclose any information relating to a child to anyone other than a person we know for certain has parental responsibility for that child.

15.1.20 Always consult with the Information Governance Officer before you develop any news ways to process personal data such as developing new electronic or paper forms, databases or spreadsheets.

15.1.21 Do not transfer personal data to any third party without prior written consent of your discipline secretary and our Information Governance Officer.

15.1.22 Do notify your discipline secretary or our Information Governance Officer immediately of any suspected security breaches or loss of personal data.

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

15.2 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 our Information Governance Officer.

16. Foreign transfers of personal data

16.1 Personal data must not be transferred outside the UK 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 we put in place adequate protections. This is mainly relevant to data held and accessed in Cloud-based services as well as some data processing the club may outsource like payroll processing or performance data analysis.

16.2 These protections may come from special contracts we need to 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 recipient's own country's laws provide sufficient protection.

16.3 You must not under any circumstances transfer any personal data outside of the UK without the prior written consent of the club Secretary or the Information Governance Officer.

16.4 We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data outside of the UK.

16.5 If you are involved in any new processing of personal data which may involve transfer of personal data outside of the UK, then please seek approval of the Secretary or our Information Governance Officer prior to implementing any processing of personal data which may have this effect.

16.6 The club's web site is operated by Team Unify and is hosted in the European data centres of Amazon Web Services (AWS). Standard contractual clauses as recognised by the Information Commissioner's Office exist in the contract between Team Unify and AWS to ensure that Team Unify is able to host information for UK-based organisations lawfully under the General Data Protection Regulation.

17. Queries

17.1 If you have any queries about this Policy, please contact either the Secretary or the Information Governance Officer.