Data Protection Policy Summary

1. Introduction

1.1 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").

1.2 This document is a summary of the main policy which can be found in the Privacy section of the web site at www.keynshamswimmingclub.co.uk

1.3 As a Representative of KASC, you are required to read and understand the full policy and you are bound by its obligations.

2. Data protection principles

2.1 The Data Protection Act 2018 and the General Data Protection Regulation set out six principles for maintaining and protecting personal data. These require that all personal data must be:

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

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

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

2.1.4 accurate and where necessary kept up to date;

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

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

2.2 We will only process personal data in accordance with the six data protection principles

3. Data subject rights

3.1 Under the legislation, individuals have certain rights in relation to their own personal data. In summary these are:

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

3.1.2 The right to have their personal data rectified;

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

3.1.4 The right to restrict processing of their personal data;

3.1.5 The right to object to receiving direct marketing materials;

3.1.6 The right to portability of their personal data;

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

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

3.2 We recognise the rights of data subjects and will uphold those rights at all times.

4. Our obligations

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

4.1.1 process personal data only for certain purposes;

4.1.2 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);

4.1.3 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;

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

4.1.5 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.

5. Your obligations

5.1 In summary, we require you to:

5.1.1 Treat all personal data with respect;

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

5.1.3 Notify your discipline secretary or the club's Information Governance Officer immediately if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to their personal data which we hold;

5.1.4 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

5.1.5 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.

6. **Practical matters**

6.1 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:

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

6.1.2 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.;

6.1.3 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.;

6.1.4 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;

6.1.5 **Always** encrypt laptops, mobile devices and removable storage devices containing personal data;

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

6.1.7 Do password protect documents and databases containing personal data;

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

6.1.9 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.

6.1.10 When disposing of any papers containing personal data, do not place these into the ordinary waste, in a bin or a skip etc. Either use a confidential waste service or have the items shredded before placing them in the ordinary waste disposal.

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

6.1.12 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.

6.1.13 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.

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

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

6.1.16 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, just first names or pseudonyms to preserve confidentiality.

6.1.17 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.

6.1.18 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.

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

6.1.20 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.

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

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

6.1.23 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.

Version date: 21 May 2020