Sudbury & District Swimming Club

Data Breach Policy

Our Policy

SDSC is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our members, associate, volunteers and committee members.

This Data Breach 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 and that efficient procedures are in place to deal with any breaches.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact the Committee of the Club

1. **What is a definition of a breach of data protection?**

1.1 Any circumstance where the personal data of an individual is lost or misplaced is defined as a breach of data

2. **Why do we have a data breach 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 any breach of data must be investigated fully and if viable sanctions or referrals put in place.

2.2 All data breaches will be recorded and these records will be kept for at least 6 years and any serious breaches will be referred to the ICO and/or SwimEngland (ASA)

2.3 As a club we are continually learning about data protection to ensure that all personal data is safe and secure.

3. **What to do is you suspect a breach.**

3.1 Any member suspecting a breach of data protection should inform the Chairman (or any other Committee member) as soon as possible of the breach and also send a written report of the breach for record keeping (email acceptable). This can be done in confidence.

3.2 Any member who knows of a breach of data and does not report this could be liable in terms of the breach and any consequent investigation

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

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

4.1.2 For the club:

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

4.1.2.2 **Civil Fines:** These can be very high and could be payable by the individual.

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 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 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 brand. Court proceedings are public knowledge.

4.1.2.7 **Loss of business:** Prospective members, participants, players, customers, 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 The Data Protection Act 1998 ("**DPA**") applies to any personal data that we process, and from 25th May 2018 this will be 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 as though GDPR and the DPA 2018 are 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 (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

6. **Key words in relation to data protection**

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, customer, prospective customer, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

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 video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and company 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 CCTV images.

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.

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. **Procedure after a breach has been reported/found**

7.1.1 A report of the breach will be completed stating as much information as possible

7.1.2 An investigation into the breach will be undertaken. This may include interviewing witnesses and other related members as to the nature of the breach

7.1.3 If the breach is not a major breach (as determined using the data protection policy) then recommendations to ensure more effective data protection will be put in place. This may lead to a changing of privacy notices to members, notices on the club website, updating of the data protection policy or other related policy changes. The report will be filled for recording purposes and discussed within the Committee of the club

7.1.4 If the breach is a major breach of data protection then this may lead to discipline action against the member and referral of the breach to the ICO. Any further action by the ICO will be undertaken on an individual case basis but could led to suspension from the club or more serious outcomes (please refer to data protection policy for possible other santions/outcomes).

7.1.5 Any individual member/s of the club whose data is implemented within the breach will be informed what data was breached and the club will work these individuals to ensure safer protection of their data.

7.1.6 Any individual has the right to dispute an outcome of an investigation into a breach of data. If this is a minor breach then the Club will form a sub-committee of at least 3 members to hear the dispute and make a formal decision on the outcome of any actions. We will always look to use sensible judgement wherever possible. This sub-committee must take place within 3 months of the original dispute.

7.1.7 In respect to a major breach of data (which has had to be reported to the ICO) the club will pass on thoughts of the disputed member to the ICO and work with the ICO to reach a reasonable and justified outcome.

7.1.8 Any possible breaches of data may need to be passed on the police or security services if asked for.

8. Your main obligations

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

8.1.1 Treat all personal data with respect;

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

8.1.3 Immediately tell the Chairman of the Club 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;

8.1.4 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

8.1.5 Immediately notify the Chairman 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 Workers regardless of their position or role in our organisation.

9. Queries

9.1 If you have any queries about this Policy please contact the Committee