

STREET & DISTRICT SWIMMING CLUB - DATA PROTECTION POLICY

General Statement of the Club's Duties and Scope under GDPR

The Club is required to process relevant personal data regarding members of staff (if any), volunteers, parents / guardians, current and prospective members as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller

Street & District Swimming Club has determined that it is not required to appoint a Data Protection Officer (DPO) under GDPR. We will however appoint a data compliance protection lead to ensure there is appropriate focus on the requirements of GDPR by the Committee who will endeavour to ensure that all personal data is processed in compliance with this Policy.

The Club recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) of 25 May 2018 and is actively working towards compliance with that directive.

The Principles

The Club shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:-

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Definitions

- The Club is 'Street & District Swimming Club'
- Parental consent, includes the consent of a guardian.
- Data Subject, an individual who is the subject of the personal data.

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual, for example, dates of birth, attendance records, meet results (this is not an exhaustive list).

Personal data may also include sensitive personal data as defined in the Act, for example relevant medical information.

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the fulfilment of a contract. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Sensitive Personal Data

The Club may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, ethnicity, criminal records and proceedings.

Rights of Access to Information

Data subjects have the right of access to information held by the Club, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the Chair. The Club will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days for access to records and 21 days to provide a reply to an access to information request.

The information will be imparted to the data subject as soon as is reasonably possible after it has come to the Club's attention and in compliance with the relevant Acts.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Club, including Safeguarding and prevention of terrorism and radicalisation

The above are examples only of some of the exemptions under the Act.

Accuracy

The Club will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the Club has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, they should notify the Chair and follow the GDPR complaints process (published online).

Data Security

The Club will take appropriate technical and organisational steps to ensure the security of personal data.

All volunteers will be made aware of this policy and their duties under the Act.

The Club and therefore all volunteers and members are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted or password protected at all times.

External Processors

The Club will take reasonable steps to ensure that data processed by external processors, for example, third party clubs or meet organisers are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it will be destroyed securely in accordance with best practice at the time of destruction.

Retention of Data

The Club will only retain data where justifiable. Some statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

The Club may store some data such as attendance records, photographs, meet results, achievements, records and marketing material indefinitely in its archive.

Author: Darren Hunter-Clarke

Date: 19th May 2018