## GDPR and Coventry swim School

Coventry Swim School is a Charitable Incorporated Organisation and is overseen by rules and regulations as directed by Swim England. As a Swim School we collect and store personal data about our swimmers and their parents (where appropriate) and staff (known as ‘members’) and as such we are subject to the General Data Protection Regulations (GDPR) from May 2018. As a Swim School, we do not have to appoint a data controller as such but the Management Committee have responsibility to ensure that we are GDPR compliant and that the various staff and volunteers in the Swim School understand their responsibilities and duties with regard to the privacy of personal data to prevent data breaches (data is accessed by unauthorised persons or lost) and to ensure that if a subject access request (SAR) is made we can find out and provide the data we have on a person accurately and within the required period of 30 days.

## Why do we collect data?

We collect personal sensitive data about our members (young and adult) to keep them safe, understand their interests and needs and make routine or rapid contact with parents/next of kin as appropriate to do so.

## How do we use the information about members?

* Data must only be used for swimming activities and is used for the following reasons:
* To manage and monitor group lists and moving between groups.
* To monitor collection of subscriptions and other relevant payments.
* To enable teachers to understand the health, dietary needs, backgrounds and interests of young people in their care so that they can tailor activities towards their needs and to ensure that they are safe whilst doing so.
* To ensure that Managers, Teachers, Poolside Helpers and volunteers can make routine contact with parents and where necessary, rapid emergency contact with parents/carers and provide accurate information to medical professionals in absence of parents.
* To record swimming achievements.
* To ensure that safety procedures are adhered to at all times and to meet requirements of accident insurance.
* To undertake DBS checks in line with safeguarding of children regulations.
* To claim gift aid donations.
* To ensure the safety of members when undertaking events and when undertaking activities with a third party organiser.
* To collate parental or adult members permissions with regards to publication of photos.

### **Data Privacy Notice and Agreements**

The data privacy notices and agreements should be provided to new members in web or paper based forms when joining the Swim School so that they are clear on what data is collected, stored and shared. Existing members will be provided with update to the notices and agreements should they arise.

## Subject access request—SAR

Members have the right to request a copy of the information that the Swim School hold about them, request to correct and remove information that the Swim School holds. Coventry Swim School must keep a record of these requests and they adopt the Swim School’s SAR process policy & procedures.

If staff receive a SAR then the subject should be asked to write to the Swim School Manager. There may be a charge of a ‘reasonable fee’ in line with the Swim School’s SAR policy & procedures.

Staff may be asked to provide, correct or delete information if a SAR is received. This must be completed within 14 days of the request as GDPR states that the Swim School must provide the information within 30 days. Some information may be redacted to comply with confidentiality.

### **Data breach notifications**

A data breach can be defined as:

* the disclosure of confidential data to unauthorised individuals
* the loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data, PCs, USBs, mobile phones; laptops, disks etc.
* the loss or theft of paper records
* inappropriate access controls allowing unauthorised use of information
* a suspected breach of IT security
* attempts to gain unauthorised access to computer systems, for example hacking
* records altered or deleted without authorisation from the data ‘owner’
* viruses or other security attacks on IT equipment systems or networks
* breaches of physical security for example forcing of doors or windows into a secure room or forcing open a filing cabinet containing confidential information
* confidential information left unlocked in accessible areas & insecure disposal of confidential paper waste
* leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
* publication of confidential data on the internet in error and accidental disclosure of passwords
* misdirected emails or faxes containing identifiable personal, confidential or sensitive data

Coventry Swim School has adata breach plan policy process. If a member of the swim School detects a suspected or actual breach they should contact the Swim School Manager for a copy of the Swim School Breach Policy & Notification Form and complete it swiftly for further analysis and response.

If a breach is assessed to be a certain severity, then the ICO (Information Commissioner’s Office) need to be made aware within 72 hours of first discovering it. Further details can be found on the ICO website.

Data breaches can result in fines of up to 4% of turnover regardless of the type of organisation.

**Management Committee Responsibilities**

The Management Committee is responsible for supplying and maintaining guidance to members within the Swim School for data capture, transfer, storage and retention.

The committee are required to oversee GDPR compliance through policies and procedure and ensure that SAR and data breaches are dealt with correctly and within the time frames identified.

## Adult Member or Volunteer Responsibilities

Adult members or those who volunteer to support the work of the Swim School whether that be working directly or indirectly with young people need to ensure that they follow best practice guidance and Swim School policies and procedures for data collection, processing and storage to maintain our GDPR compliance and avoid data breaches. Adult members or volunteers should only collect, store and use data that they need to carry out their nominated role successfully. Adult members should follow the data security best practice laid out in the Swim School guidance.

## Data collection processes

Initial queries about joining will often be by email or telephone. Data collected here should be name, date of birth, parent contact details and previous swimming experience to determine position in waiting lists. Once this data is transferred, the relevant email or paper notes should be deleted or shredded.

Personal sensitive data may be collected via paper form or via web link forms. Ideally, all data should be recorded electronically and paper forms shredded however the Management Committee recognise that some situations may have limited WIFI connections (eg on poolside) or be without computer access, in these circumstances printed copies of forms will be held by the lead person for that lesson day. In these situations appropriate secure arrangements are made for security.

Where data has to be collected for events in addition to routine activities, only that which is required should be collected, stored securely and destroyed after the event.

Where a third party requires data to be collected for safe running of activities then adult members should only provide what is necessary and where sensitive personal data is required GDPR compliance might need to be checked—please refer to the Swim School Manager. If the data is to be completed by parents on paper then these forms must be held securely before transfer to the third party.

## Data storage

Ideally, personal sensitive data should be stored electronically on the Swim School’s database however where paper based format is used the forms should be stored in locked files with keys kept separately.

All electronic devices used for storing personal sensitive data should be protected by a strong password at least 8 characters long and any USB storage devices encrypted or locked therefore requiring a password to access.

Laptops etc. should have up to date operating systems, anti-virus software and anti-malware software and ideally encryption of hard drive. Only data that is absolutely needed should be stored.

Some information is recorded on the website to allow for recording of results from events including but not exclusive to galas and this information is publicly accessible.

For many off site events paper based forms of data is the most appropriate method for staff to have personal data at hand to ensure the safety of all members. Staff should only print information that is needed for the activity, ensure that it is stored securely and then destroy once the activity is completed. Where the data has been shared through home contact system, this should be destroyed securely.

Sensitive and personal data, in most cases will only be stored for as long as it is required. Young people’s data must be deleted as soon as is practically possible and not exceeding 3 months. Some names and results may be stored for the life of the Swim School, particularly those who have qualified or participated in a high level event. It is recommended that all adult members regularly “cleanse” their data storage in whatever format they use to remove unnecessary data.

## Use of email

Emails are efficient means of communication with parents and adults linked to the Swim School but are the biggest cause of data breaches. Sending personal data via email should be limited and care taken to ensure that correct email addresses are used and BCC used for mass mailing of parents. Personal and sensitive data should not be included in the main body of the email and initials should be used where possible. If personal information is required this should be in a password protected attachment and the password given by phone upon request.

## Social Media

Personal data should not be collected, stored or shared on social media or linked direct messaging. Swim School closed Facebook accounts should only be used for general communication and updates with members and their parents.

### **Young members and GDPR**

Adult members should remind young members that they must not share personal data for themselves or others without permission to do so which includes sharing photographs or videos of Swim School activities on social media.

Policy Date: 14th April 2020 Reviewed by: Management Committee Next Review Date: Dec 2020