



AquaKidz Data Protection Policy

Purpose:

We collect data for a variety of justifiable reasons:

- As an employer to be able to manage our staff (references, ensuring safe working practices, staff absences, administration and training, monitoring staff conduct, disciplinary matters)
- Administrative of our services to customers
- Financial, regulatory and payroll duties
- Business development and marketing
- Investigating complaints
- Marketing our business
- Improving services

This Policy sets out the obligations of AquaKidz regarding data protection and the rights of its staff and customers in respect of their personal data. It details our obligations regarding the collection, processing, transfer, storage, and disposal of personal data under the General Data Protection Regulations (“GDPR”).

This policy supports our published Staff and Customer Privacy Notices which give more detail on how we process personal data.

This policy applies to all staff. You must be familiar with this policy and comply with its terms

We have not appointed a Data Protection Officer to oversee our compliance with data protection laws, as we not required to do so, but each Swim School Manager has overall responsibility for data protection compliance in our organisation. They can be contacted by emailing swim@aquakidz.co.uk.

Personal Data:

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Sensitive personal data

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy.

Data subject: the person who the data is about (i.e. the customer or the employee)

Data Controller: Pooling Better Resources Ltd (Client Management System Provider)

Data processor: AquaKidz and other identified 3rd parties

Data breach: this is when something goes wrong (loss/theft of data/human error/data shared with the wrong people/insecure disposal/verbal disclosure) with the result of causing embarrassment, distress, physical harm or financial harm

The 8 Data Protection Principles (Data Protection Act 1998)

AquaKidz and all staff who have access to or process personal information must ensure that they follow the data protection principles. Personal data shall:

1. Be obtained and processed fairly and lawfully, it will not be processed unless one of the legal conditions as set out in the legislation is met
2. Be obtained for a specified, limited, appropriate and lawful purpose, it will not be processed if incompatible for that intended purpose
3. Used in a way that is adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Kept for no longer than is absolutely necessary
6. Handled according to people's data protection rights
7. Kept safe and secure away from unauthorised access, accidental loss or destruction
8. Not transferred outside the European Economic Area, unless that country has equivalent levels of protection for personal data

The GDPR Regulations (2018)

These regulations build on existing Data Protection principles to create more accountability and enhance the rights of individuals and their privacy. With GDPR the principle of consent is key.

The 8 principles of GDPR are that data must be:

1. Fairly and lawfully processed (i.e. for good reason)
2. Processed in line with an individual's rights
3. Processed for limited purposes
4. Accurate and current (data must be erased/corrected without delay)
5. Time-limited (no longer than is necessary)
6. Legitimate and explicit (not processed for other reasons)
7. Secure and protected (accidental loss, destruction, damage, unauthorised or unlawful processing)
8. Not transferred out of EU (EEA) without adequate protection and consent

GDPR gives individuals the following 8 rights:

1. to be informed (privacy notice detailing HOW their data will be processed and by WHO)
2. to access personal data held on them via a SARs request
3. to have their data corrected if inaccurate
4. to be deleted off your systems permanently (in some situations this can be refused)
5. to block or stop their data being processed
6. data Portability (subjects can obtain and reuse their data for their own purposes)
7. to object to data processing (e.g. direct marketing)
8. to have safeguards on any Automated Decision Making (i.e made without human intervention)

Responsibilities of the Swim School Manager

- Keeping staff and customers updated on data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging staff data protection training and providing advice
- Answering questions on data protection from staff and customers
- Manage all SARs requests
- Checking and approving with third parties that handle the company's data
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy

Our procedures

ICO Registration

We are registered with the UK Information Commissioner's Office (ICO) to ensure our compliance.

Our commitment

The company will adhere to Data Protection Act and GDPR by:

- Observing the conditions regarding the fair collection and use of information
- Consent to the processing of their personal data for one or more specific purposes must be sought.
- Only collect and process appropriate information to the extent that it is needed to fulfil our operational needs and/or to comply with legal requirements
- Ensuring the quality of information that we use
- Ensuring we do not hold the information any longer than necessary
- Data will be updated promptly when a data subject notifies that it is inaccurate.
- Ensuring the rights of people of whom the information is held under the Act (e.g. informing them that processing is being undertaken, to access personal information, correct, rectify or erase incorrect information)
- Ensuring we have the appropriate technical and organisational security measures to protect personal information
- Not transferring personal information abroad without suitable safeguards being in place

Why we gather data

Generally speaking, our legal justifications for processing data will include:

1. To meet a legal obligation
2. To pursue a legitimate interest
3. Or where the data subject has consented

We will create an audit trail of consent as appropriate. We will respect privacy in all our activities

Staff Information

Staff will complete a new starter form when they join the company which provides the information necessary to comply with HR procedures. Once a member of staff leaves the company their personal details will generally be stored for up to 6 years.

Customer Information

Customers are required to complete a registration form before accessing our services. The requested information is necessary in order to carry out safe provision of our services. This information is stored centrally at the head office. We will only share this information with the Swim School which the subject is a current customer of. The AquaKidz data privacy impact assessment details of all the data processing activities undertakes.

Sensitive Personal Data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this (e.g. writing to a GP about a medical condition) unless exceptional circumstances apply, or we are required to do this by law (e.g. a DBS check). In such circumstances we will make it clear what the relevant data is, why it is being processed and to whom it will be disclosed. We must also detail the legal basis on which we are permitted to process this data.

Our Privacy Notices

Our Privacy Notices set out the purposes for which we hold personal data on both customers and employees. It also highlights that our work may require us to give information to third parties. We aim to communicate to employees and customers regular on matter regarding their privacy.

Privacy Impact Assessments:

We have mapped out all the data that we collect, process and store for both staff and customers. This ensures that our systems of data processing, retention and storage are adequate. These systems will be reviewed regularly.

Data audit and register

We will conduct regular audits to manage and mitigate risks on our data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

3rd Party Processors

We will ensure that all 3rd party processors of our customer or employee data meet our strict standards for data protection. Where necessary, legal agreements will be signed.

Subject access requests(SARS)

Any reasonable request from a data subject to access the information we hold in them will be met. We aim to providing the relevant data (as requested) in a suitable format within 30 days of the request being received in writing.

We will not charge for such requests. We will provide full disclosure in a digital format wherever possible. We can refuse or charge for requests which are excessive.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where it cannot be accessed by unauthorised personnel.
- Printed data should be shredded when it is no longer needed. This needs to be completed by a certified secure destruction service.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs, memory sticks, or similar portable media must be locked away securely when they are not being used. Data on portable media must be encrypted.
- The Swim School Manager must approve any Cloud services used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform your Swim School Manager.

Your Personal Data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform your Swim School Manager so that they can update your records.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

International data transfers

Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data security

All AquaKidz staff are responsible for ensuring:

- Data security is maintained by protecting the confidentiality, integrity and availability of personal data
- Personal information is not disclosed verbally, in writing via email or any other web pages or by any other means to any unauthorised third party

Reporting breaches

All members of staff have an obligation to report actual or potential data protection. All personal data breaches must be reported immediately to the Swim School Manager. If necessary the Swim School Manager must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

Privacy Training

All staff will receive compulsory training on this policy and the law relating to data protection. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Communications

Information will be made available to all staff regarding any changes to the data protection policy, the procedures that they will need to follow and/or how data breaches are handled. Our managers are available to answer any questions on this complicated area.

Monitoring

This policy and its procedures will be reviewed regularly for improvements. We reserve the right to change this policy at any time. This will ensure it is fit for purpose, reflects the services we deliver to our approved centres and we provide services which are relevant to the requirements of individual needs. Everyone must observe this policy. The Swim School Manager has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Swim School Manager

Statement for under 18s

We appreciate that this is a complex area. Privacy statements have been written specifically to enable under 18s to understand how their data is processed by AquaKidz. If you do not understand any other important aspects of this policy and procedure then please speak to your manager who will help to explain and provide additional age appropriate training if this is needed.

The Extent of the Policy

This Policy does not form a part of any employment contract with any employee. The Swim School reserves the right to amend and update this Policy at any time.

Please speak to your manager if you have any questions or concerns about this Policy & Procedure