DATA PROTECTION POLICY

WATERSIDE POOL
WATERSIDE COMMUNITY TRUST
CHARITY No. 1174631

1. Introduction

Data Protection legislation [currently The Data Protection Act 1998 – "DPA"] lays down certain requirements as to the collection, use and storage of Personal Data. The purpose of this document is to formalise Waterside Community Trust's ["WCT"] approach to and management of Data Protection as a Data Controller, to ensure compliance.

On 25 May 2018 the UK will adopt new Data Protection laws in accordance with the EU Directive on General Data protection ["GDPR"] (EU 2016/679). A new DPA is anticipated to refine and extend the provisions of the Data Protection Act 1998 and whilst WCT is making advance preparation for this legislation, certain review and additional amendments to this Statement will be required at that time.

1.1. Scope

This document applies to all WCT's officers, trustees and staff and also to those not employed by WCT but who are engaged to work with, or have authorised access to, WCT's information.

The document applies to all locations from which WCT's systems can be accessed including mobile and home use. Where there are links to enable third party organisations to have access to WCT's information, WCT will confirm that security policies and controls meet the required standards or that any risks are understood and mitigated.

The document applies to all Personal Data held or transmitted in paper or electronic formats or communicated verbally in face to face conversations or by telephone.

1.2. Policy Statement

WCT is responsible for a significant amount of Personal Data, relating to current and past members. The processing of this information is governed by the Data Protection Act 1998 ["DPA"].

In order to comply with the DPA, WCT as a Data Controller has a number of measures in place, details of which are defined in this document.

Responsibility for Data Protection on a day-to-day basis is everyone's responsibility, and is NOT solely the responsibility of Officers, Trustees or senior staff. Everyone must do their part to ensure that the DPA is adhered to and not breached.

2. The Data Protection Act 1998

2.1 Personal Data

Personal Data – Data which relate to a living individual (*GDPR: Natural Person)* who can be identified from that data. E.g. Name, address, date of birth.

Sensitive Personal Data (*GDPR: Special Category Data*) – data which relates to an individual and includes attributes such as: race, ethnic, political, religious, trade union, physical or mental health, sexual orientation, criminal proceedings or convictions. Such data requires additional attention to care in processing and confidentiality. For WCT this will may involve health data in relation to physical activity.

2.2 Principles of Data Protection

The DPA includes eight principles, namely that:

1. Data should be processed fairly and lawfully
2. Data should be obtained for one or more specified lawful purposes
3. Data shall be adequate, relevant and not excessive
4. Data shall be accurate and where necessary kept up to date
5. Data is not kept longer than is necessary for its purpose
6. Data shall be processed in accordance with subject rights under the Act
7. Appropriate technical and organisational measures shall be taken against unlawful or unauthorised processing, loss, destruction or damage
8. Data shall not be transferred outside the EEA unless the recipient country ensures adequate protection of protection for rights and freedoms of data subjects in relation to the processing of Personal Data

2.3 Individuals' Rights

Through Principle 6, the DPA gives individuals certain rights in relation to the use of their Personal Data. These rights enable the individual to:

- Make subject access requests regarding the nature of information held and to whom it has been disclosed
- Prevent processing likely to cause damage or distress
- Prevent processing for the purpose of direct marketing
- Be informed about the mechanisms of automated decision-making processes which may affect them
- Not have significant decisions about them taken solely by automated processing
- Claim compensation if they suffer damage by any contravention of the DPA

- Rectify, block, erase or destroy inaccurate data
- Request the Information commissioner's Office to assess whether any provision of the DPA has been contravened

2.4 Section 29 Requests

Occasionally requests may be received from authorised third parties (such as the Police) to disclose Personal Data without the need to obtain consent from the individual/s concerned. There are provisions within the DPA for such requests which in WCT's case will usually be linked to the prevention or detection of crime. Such requests can cover all data types and may include records, correspondence, CCTV footage or telephone call recordings. Currently there is no CCTV equipment at Waterside Pool.

2.5 The Information Commissioner's Office (ICO)

The Information Commissioner is an appointed person who reports directly to Parliament and is not answerable to any Minister. He/She has certain legal powers, in his/her own right, to enforce the DPA.

2.5.1 Enforcement of the DPA

Failure to comply with the DPA could result in the prosecution of an organisation or company which is a Data Controller, its officers, trustees or directors, and also of individuals concerned in the processing of Personal Data.

Data Subjects may also sue for compensation for damage and any associated distress suffered as a result of:

- Loss or unauthorised destruction of data
- Unauthorised disclosure of or access obtained to, data
- Inaccurate or misleading data

A number of tools are available to the ICO for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. These include criminal prosecution, non-criminal enforcement and audit. The information Commissioner also has the power to serve a monetary penalty on a Data Controller.

The main options are:

- To serve information notices requiring organisations to provide specified information to the ICO within a specified time period
- To issue undertakings committing an organisation to a particular course of action to improve its compliance
- To serve enforcement and 'stop now' orders where there has been a breach, requiring organisations to take (or to refrain from taking) specified steps in order to ensure compliance
- To conduct consensual assessments (audits) to check compliance
- To serve assessment notices to conduct compulsory audits to check whether good practice is being followed
- To issue monetary penalty notices requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010
- To prosecute those who commit criminal offences under the DPA

Although all the above enforcement actions are available to the ICO, possibly the greatest negative impact on an organisation following a breach would be the adverse impact on the organisation's reputation and associated publicity. All details of every enforcement action taken by ICO is made public on its website and may be broadcast by the media.

2.5.2 Registration with the ICO

Under the existing DPA all organisations that are Data Controllers are required to register with the ICO *(the GDPR will abolish this requirement once adopted into UK law after 25 May 2018 but a fee may still be payable).* The details of a notification include descriptions of the data processing carried out, the nature of Personal Data processed, and the persons or bodies to whom data may be disclosed.

3. Governance

The Trustees and Senior Management of WCT are all committed to the adoption of this Data Protection Statement and to ensuring compliance with the requirements of the DPA by all employees and those authorised to access, process and hold data.

WCT is responsible for reporting that compliance is maintained in regard to all data processing activities, and to advise, via its Board of Trustees and General Manager, on good practice. The Trustees and General Manager will regularly review such reports and advice and will consider any risks arising in order to consider any appropriate mitigation in relation to the extent to which data is processed and held.

4. Training and Awareness

As part of their induction process all new employees of WCT will receive awareness training which will include both Data Protection and Information Security processes and procedures. Employees with access to Personal Data will undergo training specific to their role. Refresher training will be provided periodically thereafter.

5. Subject Access Requests (SAR)

As noted in 2.3 above, all individuals have entitlement to access Personal Data that an organisation holds about them in both paper and electronic record format.

On receipt of a SAR, WCT has 40 days to disclose the information and any such request shall be passed to the Data Protection Officer without delay. It is currently permissible to charge up to £10 per request on satisfactory proof of an individual's identity. Any charge shall be at the discretion of WCT.

WCTis responsible for ensuring that data is disclosed in line with the requirements of the DPA. It will sometimes be the case that information requested will include Personal Data of another person. Such third-party information will not be disclosed without the consent of the third party. If it is decided that the Personal Data of the third party needs to be withheld, all information that could identify the third party will be redacted.

Where Personal Data include health records provided by a healthcare practitioner which the individual has not seen, such data will not be disclosed without the consent of the practitioner, who may withhold consent if they feel that disclosure would be to the detriment of the individual concerned.

When making the final disclosure, the following details will be provided:

- Information on whether or not the Personal Data are processed
- A description of the data, purposes and any recipients
- A copy of the data; and
- An explanation of any terminology contained within the data

6. Verification of Enquirers

Before disclosing any Personal Data (e.g by telephone, written or electronic correspondence) verification checks will be carried out to ensure that information is being provided to the correct person.

Such verification will include confirming at least two of the following details:

- Postcode or first line of address
- Data of birth
- Membership number
- Current telephone contact details held

Verification should be carried out on all telephone calls. If in doubt or in response to an enquirers' concerns, a call-back should be offered. Inbound e-mails or correspondence should also be subject to verification in any case where there is doubt about their origin.

Data will not be provided where doubt remains about the identity of the enquirer.

7. Disclosure to Third Parties

7.1 Consent

If a Member is happy for WCT to disclose Personal Data to a third party, such as a spouse, dependent or relative, they may give consent to do so. Consent may be either verbal or written but should be recorded.

The level, range and any time period of consent is determined by the Member concerned. Consent should be refreshed periodically to ensure it is still valid and such updates should be recorded.

7.2 Power of Attorney POA)

It may occur that an individual has POA for a Member. It is reasonable for WCT to verify that this is so before allowing the person with POA to access a Member's Personal Data.

8. Third parties

8.1 Disclosures

WCT does not routinely disclose Members' Personal Data to third party organisations nor does it undertake direct marketing on behalf of any such organisation.

Personal Data is disclosed only under the following circumstances:

- Members who are involved in swimming lessons or training activities under WCT's authority or management shall permit their Personal Data and any health data (only in so far as it is relevant and necessary) to be disclosed to the Teacher or to authorised and appointed training instructors for use solely in connection with their roles
- In the case of a Minor Personal Data will be released to the School or other appropriate Safeguarding Officer in the event of any Safeguarding issue requiring reporting in line with WCT's Safeguarding Policy

8.2 Data Processing

Data may be held (hosted) and processed on WCT's behalf by third party processors as necessary for the performance and administration of WCT's responsibilities. WCT has taken steps to ensure that all data is hosted within the EEA and is subject to appropriate Data Protection requirements in regard to processing, security and confidentiality. Such systems include:

- Race and Swimming Gala Results management (Ryde Swimming Club)
- Swimming Lesson bookings (ThinkSmart Software Ltd)
- Aerobic/Dance/Waterworkout or similar sessions (ThinkSmart Software Ltd)
- Finance administration (Xero - data stored by Amazon Web Services, USA)
- Financial data (Barclays PLC)

9. CCTV

WCT does not operate a CCTV system