Data Protection Policy

POLICY MANAGEMENT:

This policy was adopted by the Committee on: 12 June 2013

Introduction

Everyone has rights - with regard to how their personal information is handled. During the course of our activities we (WDSC) will collect, store and process personal information about our members, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of names, addresses, medical and information regarding membership payments of members and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

Policy

This policy – in line with ASA guidelines - sets out WDSC rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

As a not-for-profit organisation WDSC may process sensitive personal data for internal purposes. The processing of sensitive data for any other purpose (including, for example, disclosing sensitive personal data to a third party such as another swimming club) will require the express consent of the person concerned.

Definitions

Data

Information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects

For the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a member of WDSC or a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data

Data relating to a living individual, who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a swimmer's report at the end of a term).

Data controllers

The people or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

The Club is the data controller of all personal data used for the purposes of running WDSC.

Data users

Includes all volunteers whose work for WDSC involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors

Includes any person who processes personal data on behalf of a data controller, it could, for example, include other swimming clubs with which WDSC organises swimming galas.

Processing

Is any activity that involves use of the data; It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data

Includes information about a person's racial or ethnic origin, physical or mental health or condition, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings (This information may be in the possession of the club's welfare officer following a volunteer's application for a CRB check). Sensitive personal data can only be processed under strict conditions.

Data protection principles

Anyone processing personal data for WDSC must comply with the eight enforceable principles of good practice. These provide that personal data must be:

1. Processed fairly and lawfully

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case WDSC), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met.

If sensitive personal data is to be processed for any other than WDSC's internal purposes (including disclosing sensitive personal data to a third party such as other swimming clubs), the data subject's explicit consent to the processing of such data will be required.

2. Processed for limited purposes and in an appropriate way

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed (if, for example, WDSC extends its activities), the data subject must be informed of the new purpose before any processing occurs.

3. Adequate, relevant and not excessive for the purpose

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject (i.e. WDSC's activities). Any data which is not necessary for that purpose should not be collected in the first place.

4. Accurate

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

5. Not kept longer than necessary for the purpose.

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

6. Processed in line with data subjects' rights.

Data must be processed in line with data subjects' rights. Data subjects have a right to:

1. Request access to any data held about them by a data controller.
2. Prevent the processing of their data for direct-marketing purposes.
3. Ask to have inaccurate data amended.
4. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. Secure

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he/she agrees to comply with those procedures and policies, or if he/she puts in place adequate measures himself/herself.

8. Not transferred to people or organisations situated in countries without adequate protection.

This means we must take check before sending any personal data abroad (eg to overseas clubs).

Personal data should not be stored on any website or cloud based facility that does not provide adequate protection (always read the T&Cs)

Data security

WDSC will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

1. "Confidentiality" means that only people who are authorised to use the data can access it.
2. "Integrity" means that personal data should be accurate and suitable for the purpose for which it is processed.
3. "Availability" means that authorised users should be able to access the data if they need it for authorised purposes.

Some Examples of Personal Data we use

This list is not exhaustive:-

- Membership information, Names, addresses, contact numbers

- Billing Information
- Swimmer details, typically stored on the Hytek Team Manager Database and any back up copies
- Gala Information, including meet manager and historical meet files
- Contact Lists
- Swimmer performance data
- Medical Information
- Digital video and photographic information obtained for the purposes of coaching.

Security procedures

Entry control

Any stranger seen to be trying to obtain any personal data (e.g. by trying to get access to registers etc.) should be reported.

Safekeeping

Registers and any other materials containing confidential information should always be kept safe. (Personal information is always considered confidential.)

Methods of disposal

Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

Data Storage

Personal data should only be stored on our central data base or club computers. Personal data should not be stored on individuals home PCs and only printed or copied as strictly necessary. Old computer disks, USB drives and hard drives from club laptops, should be destroyed.

Data Transfer

Personal Data Should not be sent by email, memory stick or any other unsecure method unless encrypted.

Dealing with subject access requests

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any volunteer who receives a written request should immediately forward it to the secretary.

Providing information by Email

Anyone dealing with emails and personal data should be careful to limit the information to the minimum that is required.

1. Do not send unencrypted club databases containing personal data by email (except where permission exists for that purpose e.g. Hytek entries).
2. Ensure that only required data is sent and only sent to those who should have it (e.g. owner, data controller). Can it be avoided; most personal data is already held on our files.
3. Ensure that emails containing personal data are not forwarded or replied to without removing personal data.
4. Delete (fully delete from deleted items) emails containing personal data when the data is no longer required.
5. Refer to the Chairman or Welfare Officer in difficult situations. No-one should be bullied into disclosing personal information.

Providing information over the telephone

Anyone dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

1. Check the caller's identity to make sure that information is only given to a person who is entitled to it.
2. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
3. Refer to the Chairman or Welfare Officer in difficult situations. No-one should be bullied into disclosing personal information.

Declaration

I have read and agree to abide by the procedures as described in the above Policy. I understand that I should not disclose any password (which gives me access to the club data) to any third party, and that - should I do so – I will be the subject of disciplinary action by the club.

Signed:…… Date…….