WATERLOO
NETBALL

Principles

This policy applies to all personal data collected and processed by Waterloo Netball. It defines the how Waterloo Netball manages and controls the data of individuals. All persons who handle personal data on behalf of the organisations must read and confirm acceptance of the principles it defines.

Types and Categories of Data

The types and categories of data collected, stored and processed are as follows:

- Identifiers, such as name, email address, social media Ids, mailing address, IP addresses, MAC addresses, cookies, and telephone numbers.
- Personal characteristics: gender, age, date of birth.
- Correspondence exchanged with the data subject.
- Bank account numbers and payment details.
- Health information and details of medical conditions.
- Information pertaining to children (under 16).

Legitimate Uses

Except where required by law or to protect the specific interests of an individual, data may only be used for the purposes specified and notified to the data subject when it was obtained.

The general privacy notice should reference these data uses and other specific notifications should be given to individuals where appropriate.

Correspondence with club members and the public using their identifiers is permissible on the grounds of legitimate interest as it is something any person would reasonably expect an organisation to do.

General (non-essential) information can only be sent directly to subscribers who consent to receive such material.

Club members consent to their personal characteristics (age, gender etc.) being used for the purpose of organising training, events, activities and competitions.

Known medical conditions and health information may only be used for the specific purpose of protecting the health and well-being of the individual. This information may only be provided by consent of the individual or parent / guardian.

Cheques, bank details and other payment information is used in financial transactions between individuals and the organisation. No formal consent is required to process such information as this is a legitimate use which one would reasonably expect.

Retention

Except where so required by other overriding laws and compliance obligations, information will be deleted in accordance with this schedule:

- 3 months after an individual ceases to be a club member.
- When explicitly requested by the individual. This may necessitate termination of membership.
- Information which is not required for the effective running of the club will be deleted after 3 months.

Non-essential correspondence which may exist in individual club officers' accounts or in 3rd party communication services must be deleted as soon as practically possible after 3 months.

Location and 3rd Parties

All personal data should be stored in a suitable data management service to which specific officers of the organisation are granted access.

No personal data should be stored on officers' personal computing devices or in their own communication accounts.

The only exception to this is where information is being uploaded into the central storage or where incidental correspondence is taking place on behalf of the organisation.

Personal data in hard-copy form or temporarily held on personal computing devices should be uploaded to the central data store as soon as practically possible and then deleted from the temporary locations. Hard copies should be appropriately destroyed, e.g. by shredding.

3rd party services used for data storage and processing should comply with data protection legislation and provide the organisation with a statement of their policies for protection of data.

Data services should be located within the EEA, an approved country or operate appropriate security and procedural controls to protect data.

Security Controls

By using an approved central data store, there is less risk of data being compromised through security deficiencies in the organisation's officers' personal computing devices.

Only those officers who require access to individuals' data should be granted access and the access list should be reviewed on a regular basis. Access should be removed as soon as an officer leaves their position.

Officers may temporarily store personal data on their own computing devices, solely for the purpose of uploading this to the central management system. Personal computing devices should have anti-malware software installed and all programs should be kept updated with any vendor supplied patches.

A separate security policy defines the measures the organisation should take to protect all of its information, including personal data.

Records

This policy and the accompanying privacy notice record the types of data collected and their intended use.

A record needs to be kept of the consent provided by an individual. The most appropriate way to achieve this is to upload a scanned copy of the individual's membership application form and destroy the original.

A record needs to be kept of any use of health information. Its initial provision and subsequent storage in the central data management system is recorded by retaining the electronic copy of the membership application form.

Any subsequent use of this data should be separately recorded, stating clearly when the data was used and why it was necessary.

Procedures

Individuals may request a copy of the information the organisation holds about them. Following such a request, an officer with access to the data management system should export a copy of the information in a suitable electronic form within 30 days.

Appropriate safeguards should be used to protect the information provided to the requesting individual.

If the data management system allows members to log in, an online record of the data exported should be provided within the user's login account.

The exported data can be compressed, encrypted and emailed directly to the data subject from the data management system, with the decryption password provided separately.

If an individual advises the organisation of changes to the data it holds, an officer should amend the details in the central management system. A record of this amendment should be kept, ideally through automatic means.

If an individual requests that their data is deleted, the organising committee or data protection officer should determine what information can be deleted and what needs to be retained in order to comply with other legal obligations. If necessary, the data may be archived rather than deleted, if such a mechanism exists.

If there is no reason to retain the data, it should be deleted and a record kept of the deletion action.