



Data Protection Policy

Contents

1	Introduction	2
2	Purpose of this policy.....	3
3	Canoeing Ireland Data usage statement	3
4	Data Protection Principles	4
5	Responsibility	5
6	Data Security.....	5
7	International Transfers	6
8	Practical Pointers	6
9	Dealing with Subject Access Requests.....	6
10	Procedures and Guidelines	7
11	Review.....	7

1 Introduction

Canoeing Ireland (CI) is committed to protecting your privacy and complying with the Irish Data Protection Commissioner's guidelines. This Statement of Data Protection applies to how Canoeing Ireland manages and governs personal data collection and usage. By agreeing to these terms, you consent to the data practices described in this statement.

Privacy and data protection rights are very important to canoeing Ireland. As such Canoeing Ireland operates under the Data Protection Acts 1988 - 2003 and all personal data will be maintained in accordance with the obligations of these acts. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The Data Protection Acts 1988 and 2003 (the "Data Protection Acts") lay down strict rules about the way in which personal data and sensitive personal data are collected, accessed, used and disclosed. The Data Protection Acts also permit individuals to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect.

The types of personal information that CI may be required to handle include information about:

- Members, present and past, and where applicable their guardians.
- Current, past and prospective employees, officers, board and committee members, volunteers, CI representatives, advisers, consultants, contractors and agents.
- Registered athletes being individuals who are members of National Programmes or who compete and represent Ireland at a national level.
- Those individuals who have undertaken training or qualifications through CI or partner organisations.
- Coaches, Instructors and course providers registered with CI.
- Suppliers and sponsors; and others with whom it communicates.

The personal 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 Acts 1988 - 2003 and other regulations. The Acts impose restrictions on how CI may process personal information and a breach of the Act could give rise to criminal and civil sanctions as well as negative publicity.

This document outlines Canoeing Ireland's policy to help ensure that we comply with the Data Protection Acts. Inquiries about this Data Protection Policy should be made to: General Manager, Canoeing Ireland, Irish Sports HQ, National Sports Campus, Blanchardstown, Dublin 15.

2 Purpose of this policy

This policy is a statement of Canoeing Ireland's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transporting and storage of personal information.

This policy is a condition of employment and therefore any employees, in addition to all others who obtain, handle, process, transport and store personal information including board members, committee members, volunteers, CI representatives, advisers, consultants, contractors and agents will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action. Negligent or deliberate breaches could also result in personal criminal liability.

Any employee, board members, committee member, volunteer, CI representative, adviser, consultant, contractor or agent who considers that the policy has not been followed in respect of personal information about themselves or others should raise the matter with the CI General Manager in the first instance.

3 Canoeing Ireland Data usage statement

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected, which may include, but is not limited to,

1. The collation of data to produce statistics which will be supplied to, amongst others, government agencies.
2. To research, develop and manage new and existing programmes or projects for the strategic development of paddlesports and for promoting paddlesports generally.
3. For communicating with individuals about their membership and/or their involvement in programmes, projects, competitions, courses and other activities including the promotion of all Canoeing Ireland activities.
4. Providing information to individuals about matters related to paddlesports, activities regarding paddlesports administration and its sponsors or for any other purposes specifically permitted by the Acts.
5. Record certification, course participation, event participation, membership and to provide instructor data on the website.
6. Use of name and address data for identity verification, anti-fraud and anti-money laundering services.
7. To perform accounting and other record-keeping functions.
8. To provide personnel, payroll and pension administration services.

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, the data subject must be informed of the new purpose before any processing occurs.

4 Data Protection Principles

We shall perform our responsibilities under the Data Protection Acts in accordance with the following eight Data Protection principles:

Obtain and process information fairly

We shall obtain and process personal data fairly and in accordance with statutory and other legal obligations.

Keep it only for one or more specified, explicit and lawful purposes

We shall keep personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes as defined in the Canoeing Ireland data usage statement.

Use and disclose only in ways compatible with these purposes

We shall use and disclose personal data only in circumstances that are necessary for the purposes for which we collected the data.

Keep it safe and secure

We shall take appropriate security measures against unauthorised access to, alteration of, disclosure or destruction of personal data and against its accidental loss or destruction.

Keep it accurate, complete and up-to-date

We adopt procedures that ensure high levels of data accuracy, completeness and that data is up-to-date.

Ensure it is adequate, relevant and not excessive

We shall only hold personal data to the extent that it is adequate, relevant and not excessive.

Retain for no longer than is necessary

We shall only hold onto data for as long as it is required by the Canoeing Ireland data usage statement.

Give a copy of his/ her personal data to that individual, on request

We adopt procedures to ensure that data subjects can exercise their rights under the Data Protection legislation to access their data. Access to data is available upon a written request and on payment of the appropriate fee of €6.35. Request should be made by post to Canoeing Ireland, Irish Sports HQ, Blanchardstown, Dublin 15 or by email to the general manager at office@canoe.ie.

5 Responsibility

Overall responsibility for ensuring compliance with Data Protection Acts rests with Canoeing Ireland. However, our responsibility varies depending upon whether we are acting as either a data controller or a data processor. All employees and contractors of Canoeing Ireland who separately collect, control or process the content and use of personal data are individually responsible for compliance with the Data Protection Acts. The Data Protection Co-Ordinator is Canoeing Ireland's General Manager, and co-ordinates the provision of support, assistance, advice, and training within Canoeing Ireland to ensure that the company is in a position to comply with the legislation.

6 Data Security

CI must 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. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. The Acts requires CI 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. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:-

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the CI central computer system instead of individual PCs.

Security procedures include:

Log-on system. All IT systems have a log on system which allows only authorised personnel access to personal data. Passwords on all computers are changed frequently and must not be disclosed to others.

Secure lockable desks and cupboards. Desks, cupboards and rooms are kept locked if they hold confidential information of any kind and can only be accessed by certain individuals. (Personal and financial information and child protection data is always considered confidential and additional security measures are in place for such information.)

Methods of disposal. Paper documents should be shredded. Electronically stored information should be physically destroyed when no longer required.

Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

7 International Transfers

Personal data should not be transferred to a country outside the European Economic Area unless the country to which the personal data is being transferred provides adequate safeguards. In many cases this will necessitate the data subject consenting to the personal data being transferred.

8 Practical Pointers

To maintain data security and compliance with the law, data users should:

- When sending emails to more than one data subject (whether by a distribution list or otherwise), consider 'blind copying' each data subject so that each data subject's contact details are not disclosed to the other data subjects.
- Ensure that no information is published on the CI website in respect of a data subject unless the information is already in the public domain or that data subject has been informed and it is reasonable to do so or they have consented to such publication. Exercise care when disclosing information about someone else. Only do so if the other person has consented or it is reasonable in all the circumstances to comply with the request without the consent of the other person.

9 Dealing with Subject Access Requests

A formal request from a data subject for information CI holds about them must be made in writing. Employees, board members, committee members, volunteers, CI representatives, advisers, consultants, contractors and agents who receive a written request should forward it to the General Manager immediately. CI should respond to the request within 40 calendar days and has the right to charge a fee (presently no more than €6.35) for this service.

When receiving telephone enquiries, employees, volunteers, board members, committee members, CI representatives, advisers, consultants, contractors and agents should be careful about disclosing any personal information held on CI systems. In particular they should:

Check the caller's identity to make sure that information is only given to a person who is entitled to it. A common sense approach should be taken when verifying the identity of the caller. For example, if you personally know the individual and are satisfied that they are calling this ought to be sufficient. If you do not know the caller, you could ask to return their call and ensure that the number given tallies with that on the membership database record for the person.

Suggest that the caller put their request in writing where the employee, board member, committee member, volunteer, CI representative, adviser, consultant, contractor or agent is not sure about the caller's identity and where their identity cannot be checked. Alternatively, the individual should be asked to attend in person (and especially if the information is of a sensitive nature).

Refer to the General Manager for assistance in difficult situations (for example, where any request might involve disclosing someone else's personal data). Employees, board members, committee members, volunteers, CI representatives, consultants, advisers, contractors and agents should not be bullied into disclosing personal information.

10 Procedures and Guidelines

Canoeing Ireland is firmly committed to ensuring personal privacy and compliance with the Data Protection Acts, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

11 Review

This Data Protection Policy will be reviewed regularly in light of any legislative or other relevant developments.

This Data Protection policy is available on the Canoeing Ireland website.

Canoeing Ireland welcomes your comments regarding this Statement of Data Protection. If you believe that Canoeing Ireland has not adhered to this Statement, please contact Canoeing Ireland at info@canoe.ie. We will use commercially reasonable efforts to promptly determine and remedy the problem.