Irish Society of Chartered Physiotherapists

Privacy Statement

1. Purpose

This policy outlines how the Irish Society of Chartered Physiotherapists (ISCP) ('we') handle and use your personal information and informs you of your rights in relation to that information. Under the General Data Protection Regulations (GDPR) of May 2018, the ISCP is the controller of the personal data we collect.

The ISCP is committed to protecting and respecting your privacy. This Privacy Policy explains why and how we use the personal information we obtain from you or others, who we share it with, and the rights you have in connection with how we use your information. Please read this policy carefully to understand our practices.
This policy describes how we handle personal information collected from various interactions with you, engage with us on social media, browse our website located at www.iscp.ie, or contact us through other means.

As the data controller, the ISCP determines the purpose and means of processing your personal information. For further details, including our contact and legal information, please see the end of this policy.
This policy was last updated on 12 March 2025.

2. The Information We Process

We collect information about you in the course of operating the ISCP, which allows us to provide our services to you. We collect Personal Data from you through the use of application forms, payments, online services, phone calls and when you email your Personal Data to us. We only collect personal information that is necessary and relevant for the purposes outline below.

The types of data we collect include:

- Personal Data: This is data that identifies you or can be used to identify or contact you and may include:
  - your contact details (email address, phone, postal and work address);
  - birth date, occupation, employer, qualification, CORU registration number;
  - marketing preferences;
  - information provided in member surveys, or entries into competitions we run;
  - details of transactions between you and us;
  - payment card details, and in case of refunds, bank account details.
- Sensitive Data: If we process any sensitive personal information, we will restrict access to and use of this. Any Sensitive Personal Data that we process will be used solely for providing you with the required services.

Information We Automatically Collect When You Visit Our Site:

- Details of how you use our website, including traffic data, weblogs, statistical data, and the specific parts of the site you clicked on.
- Date, time, and duration of your website visit.
- Pages visited and time spent on each.
- The website address from which you accessed our site.
- Information on when and how you consented to receive marketing communications from us.
- Cookie, pixel, and beacon identification information (see our Cookie Policy for more details).

If the purpose of processing is for a reason other than the reasons outline above, we will seek explicit consent.

3. Use of Your Personal Information

By sending your Personal Data to us, or purchasing our services, you signify your consent to your Personal Data being used and processed by us.

We use your personal information for various purposes, relying on different legal grounds depending on the context and the associated privacy risks.

We use your personal information in the following ways:

3.1 Where You Have Provided Consent

We may process your personal information for the following purposes, provided you have given us consent:

- To contact you, in connection with the provision or services, or respond to any communication you might send to us.
- To contact you via email, online, or by post (as indicated) with marketing information about our services.
- You may withdraw your consent for us to use your information in these ways at any time. For more details, see the Your Rights in Relation to Your Personal Information section below.

3.2 Where Necessary to Comply with Our Legal Obligations

We will use your personal information to meet our legal obligations, including:

- To determine eligibility for membership.
- Keeping records related to the exercise of your rights concerning our processing of your personal information.
- Taking necessary actions regarding health and safety incidents as required by law.
- Handling and resolving any complaints we receive related to our services.

3.3 Where Necessary for Us to Pursue a Legitimate Interest

We may process your personal information when necessary to pursue our legitimate interests as a business for the following purposes:

- To provide you with professional and administrative services.
- For analysis and insights to inform our marketing strategies and enhance your visitor experience.
- To identify and record your engagement with our Site, social media, and electronic communications (please refer to our Cookie Policy for details).
- To support you with your inquiries and respond to your correspondence and requests. Including 'contact us' option on the website.
- To analyse and improve our products and services, ensuring a better experience on our Site.
- To conduct research, including member surveys, to better understand you as a member.
- To operate the administrative and technical aspects of our business effectively.
- To administer our Site and social media pages for internal operations, including troubleshooting and testing.
- For fraud prevention and other criminal activities.
- To verify the accuracy of the data we hold about you and enhance our understanding of you as a member or visitor.
- For network and information security, protecting your information against loss, damage, theft, or unauthorized access.
- To comply with requests related to your rights.
- To improve the efficiency and accuracy of our databases and systems by consolidating records.
- To enforce or protect our legal rights or to bring or defend legal proceedings.
- To inform you about updates to our terms, conditions, and policies.
- For general administration, including managing queries, complaints, and sending service messages.

3.4 Where Necessary for Us to Perform our Contract with you

We will use your personal information where necessary to perform our contract with you, for the following purposes:

- To process your payment card or bank details when taking payment for your membership or providing refunds.

- To run our competitions and promotions that you enter and to distribute prize

3.5 Marketing Communications

If we have requested your consent and you provide it, we may use your personal information to contact you by email, online, or by post regarding special offers, promotions, competitions, or new products and services.

If you do not wish to receive communications from us, please inform us by using the unsubscribe link in our emails, by sending an email to jenniferallen@iscp.ie, or by changing your preferences on your member dashboard.
If you opt out of receiving marketing communications, we will retain your email address on our suppression list indefinitely to ensure we respect your preferences.

4. How We Obtain Your Information

We obtain your personal data from the information you give to us.

5. How We Use Your Information

We will process the information you provide in a manner compatible with the GDPR. We will endeavour to keep your information accurate and up to date, and will not keep it for longer than is necessary.

We are required to retain information in accordance with the law, such as information needed for insurance, claims, cover verification and audit purposes.

All employees (not already covered by a professional confidentiality code) sign a confidentiality agreement that explicitly makes clear their duties in relation to handling personal information and the consequences of breaching that duty.

9. Disclosure of your Information

We only share your personal information outside of our organisation in specific circumstances. When we do so, we will establish a contract that obliges recipients to protect your personal information, unless we are legally compelled to disclose such information. Any contractors or recipients engaged by us will be required to adhere to our instructions. We do not sell your personal information to third parties.

We will disclose your Personal Data if we believe, in good faith, that we are required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order, or other statutory requirement.

We may when requested disclose membership status (current member or former member, not a member).

In accordance with European Directive (2005/36/EC) on the Recognition of Professional Qualifications, the ISCP is obliged to exchange information regarding disciplinary action or criminal sanctions taken or any other serious circumstances, which are likely to have consequences for pursuit of activities under this Directive.

Personal data may be used in a number of circumstances such as:

- The furnishing of information relating to the good standing of a member of the Society to the Irish Government Agencies/Foreign Government Agencies/Professional bodies, including recording information with regard to conduct or professional indemnity of that member, the context in which the information was required is almost exclusively in the context of refinement or appointment to posts or positions. This information is automatically required of all overseas applicants and E.U. Legislation will regard a practice that does not require the same information of all applicants for membership as discriminatory

We may disclose your information to our third-party service providers, course providers, agents, and subcontractors (referred to as "Suppliers") for the purpose of delivering services to us or directly to you on our behalf. This includes the operation and maintenance of our website and social media pages.

When engaging Suppliers, we only provide them with the personal information necessary for them to deliver their services. This disclosure occurs only when we have a contractual agreement in place that mandates them to keep your information secure and restricts their use of it to our specific instructions.

10. Transfer of your Personal Information Outside of Europe

Information you provide to us is stored on our secure servers located within the European Economic Area (EEA).

There are appropriate measures in place to safeguard data that is transferred outside of Europe. Appropriate safeguards are implemented for transfer and storage, as required by applicable law.

In the event that we transfer your personal information to the United States of America, we will only do so to entities that are subject to Standard Contractual Clauses or where we have alternative safeguards in place, in accordance with applicable law. Where relevant to our data transfer activities, we may rely on adequacy decisions issued by the European Commission regarding certain countries for data transfers outside the EEA.

11. Security and Links to Other Websites

We take the security of your personal information very seriously and employ a variety of measures in line with industry best practices to protect it. However, please be aware that transmissions over the internet to our website and social media pages may not be completely secure, so we advise exercising caution. When you access links to other websites, the privacy policies of those websites, rather than ours, will govern your personal information.

We implement security measures to safeguard the personal information you provide, preventing unauthorised access, unlawful processing, and accidental loss, destruction, or damage.

We utilise internet standard encryption technology ***(Transport Layer Security TLS)*** to encrypt personal data that you send to us when placing an order through our website. To verify that you are in a secure section of our site before sending personal information, please check the bottom right of your web browser for an image of a closed padlock or an unbroken key.

While we strive to protect your personal information, please note that the transmission of information via the internet is not entirely secure. Although we will do everything in our power to ensure your information is secure, we cannot guarantee its safety during online transmission. You acknowledge the inherent security risks associated with using the internet and agree not to hold us liable for any security breaches unless we are at fault.
If you are using a computer or terminal in a public setting, we recommend that you always log out and close your web browser at the end of your online session to enhance your security. Additionally, we suggest adopting the following security measures to improve your online safety:

- When creating a password, we recommend using at least 8 characters that include a combination of letters and numbers.
- We suggest frequently changing your password.
- Keep your passwords confidential. Remember, anyone who knows your password may access your account.
- Avoid using the same password for multiple online accounts.

- We will never ask you to confirm any account or credit card details via email. If you receive an email purporting to be from us requesting such confirmation, please ignore it and do not respond. Instead, report it to us.

Our website and social media pages may contain links to other websites operated by third parties that we do not control. This policy does not apply to those external websites, so we encourage you to review their privacy policies. We specifically disclaim any responsibility for their content, privacy practices, and terms of use, and we make no endorsements, representations, or promises regarding their accuracy, content, or completeness. Your disclosure of personal information to third-party websites is done at your own risk.

The material contained on our website is for general information purposes only and does not constitute professional advice covering any specific situation.

8. Your Rights

You have specific rights concerning your personal data, and we have established processes to enable you to exercise these rights

8.1 Right of Access
This right is commonly referred to as a Data Subject Access Request (DSAR). If you wish to know whether we are processing personal data relating to you and to access such data, you can email data@iscp.ie. To provide you with a copy of the personal data we hold, we will need to verify your identity.
You have the right to access any personal information that the Irish Society of Chartered Physiotherapist processes about you and to request information regarding:

- What personal data we hold about you
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom your personal data has been or will be disclosed
- The intended duration of storage for your personal data
- If we did not collect the data directly from you, information about the source

8.2 Right to Rectification
If you believe that we hold any incomplete or inaccurate data about you, you have the right to request that we correct and/or complete this information. We will endeavour to make the necessary changes as quickly as possible, unless there is a valid reason for not doing so, in which case you will be notified.

If you wish to update any inaccurate personal data we hold about you, you can do so directly by logging into your member dashboard at www.iscp.ie or contact info@iscp.ie. Depending on the nature of the personal data you believe is inaccurate, we may request further proof to ensure that the correction is made appropriately. If we are satisfied that the personal data is indeed inaccurate, we will make the necessary amendments.

8.3 Right to Erasure
You also have the right to request the erasure of your personal data or to restrict processing (where applicable) in accordance with data protection laws, as well as to object to any direct marketing from us. Where applicable, you have the right to data portability of your information and the right to be informed about any automated decision-making we may employ.

You can request the erasure of your personal data under certain circumstances. However, this right does not apply where we are required to comply with a legal obligation or where we need your personal data for the establishment, exercise, or defence of legal claims. Additionally, if you opt out of marketing communications, we must retain a record of your opt-out preference to ensure that we do not contact you in the future.

8.4 Right to Restriction

You have the right to request that the processing of your personal data is restricted under certain circumstances. However, we will still process the personal data for storage purposes, for the establishment, exercise, or defence of legal claims, or with your consent.

8.5 Right to Object
Where we are relying on legitimate interests as a legal basis for processing your data, you have the right to object to such processing on grounds relating to your particular situation.

8.6 Right to Portability
In certain circumstances, you may request that we provide your personal data to you in a commonly used format. If you wish to make such a request, please email *data@iscp.ie*.

8.7 Right to Complain to the Supervisory Authority
You have the right to lodge a complaint with the Data Protection Commission.

- Online at How to contact us | Data Protection Commissioner
- By Phone 01765 0100 / 1800 437 737 (Monday – Friday)
- By Post, 21 Fitzwilliam Square South, Dublin 2, D02 RD28

For additional information or to exercise your data protection rights, please contact us using the details provided above.

If you are unhappy with how your personal data has been used, please contact us as per contact details below.

If you wish to object to our use of your personal data for marketing purposes, we will opt you out of such communications. You can do this by logging into your member dashboard to amend your preferences, or by emailing us at jenniferallen@iscp.ie.

If we receive a request from you to exercise any of the rights mentioned above, we may ask you to verify your identity before proceeding with the request; this is to ensure that your data remains protected and secure.

Some of these rights only apply in certain circumstances and so are not guaranteed or absolute rights. If you have any queries or concerns about your rights, contact the Practice Data Protection Officer. If you are not satisfied you can contact the Data Protection Commission.

11. How Your Records are Stored

We are committed to ensuring that your information is secure. We have a number of security precautions in place to prevent the loss, misuse or alteration of your information. All employees have a duty to keep information about you confidential.

13. Retention Period

We are required to retain certain information to ensure accuracy, maintain the quality of our services, and for legal, regulatory, fraud prevention, and legitimate business purposes.

If you disclose personal data to us via a general enquiry on our website—such as by filling out a form or sending us an email—this personal data will be retained for a period of 12 months.

Other information will be held for no longer than necessary for the purposes for which it was collected or as required or permitted for legal, regulatory, fraud prevention, and legitimate business purposes. Generally, we (or our service providers acting on our behalf) will retain this information for a period of seven years, unless a longer retention period is mandated by law or applicable regulations.

We will not keep your personal information in a format that allows identification for longer than is necessary for the purposes for which we collected it. For certain purposes, we may retain your personal information indefinitely (for example, to suppress marketing messages)..

14. Payment Card Industry Data Security Standard

In line with best practice, members' credit card details are stored by Global Payments. Global Payments is fully compliant with the Payment Card Industry Data Security Standard ("PCI DSS") which is the standard required by banks and credit card companies for card storage and processing.
Members account details for direct debit payments are stored by GoCardless. GoCardless is ISO 27001 certified for information security. GoCardless global data risk management programme is built to GDPR standards and applies privacy best practices to help protect and respect personal data.

15. Changes to our Privacy Policy and Contact Details

Please check this page regularly for any changes to this policy. You can contact us with any queries related to this policy or for any other reason by post, email, or phone.

Please email us at info@iscp.ie or call us on +353 1 402 2148.

You can also contact our Data Protection Officer, Marie Ó Mir at *data@iscp.ie* .

Please contact our data protection officer:

- If you have any queries in relation to Data Protection or other issues around the security of your personal information,
- For more information about the steps, we take to protect your information,
- For more information about your rights, including the circumstances in which you can exercise them and how to exercise them,
- If you wish to raise a complaint on how we have handled your personal information.

The Data Controller is: The Irish Society of Chartered Physiotherapists, 13 Adelaide Road, Dublin 2, D02 P950, Ireland, info@iscp.ie, +353 1 402 2148.

Approved	March 2025	
Board approved	Not applicable	
For Review	March 2026	
Other Documents superseded by this one	Privacy statement 2022	
Access to Document	All	
Location of Document	Website and Inventory of Documents	
Related Documents	○ Cookie policy	