Privacy Policy

IFS Wealth & Pensions Ltd

Version 4.2 | July 2026

Data Controller

IFS Wealth & Pensions Ltd

FCA No. 713063

info@ifswp.co.uk

Your right to privacy is important to us. This policy explains your privacy rights and how IFS Wealth & Pensions Ltd collects, uses, manages and stores your personal data, and how your rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 are upheld.

We collect information about you so we can carry out the services we have been contracted to provide. We will only share your personal data in the circumstances set out in this policy.

Who is responsible for your data?

IFS Wealth & Pensions Ltd (FCA Register Number: 713063) is the Data Controller in respect of personal data we hold about you. This means we are responsible for deciding how and why your personal data is processed.

If you have any questions about how we use your personal data, please contact Ricky Chan at info@ifswp.co.uk or by post at: Thomas House, 84 Eccleston Square, Victoria, London, SW1V 1PX.

Personal data we collect about you

The type of personal data we collect about you and how it is used depends on what contact you have with us, your needs, the relationship you have with us, and the products and services you hold or enquire about. The following is information which we will typically need to obtain:

- Title, name, date of birth, marital or civil status, gender, contact details, addresses, and nationality. This also extends to documents that will help us verify your identity.
- Employment and remuneration information, including salary, bonus schemes, overtime, sick pay, other benefits and employment history.
- Bank account details, loans and other liabilities, tax information, income and expenditure, family circumstances and details of any dependants.
- Health status and history, details of treatment and prognosis, and medical reports (where relevant to protection advice).

We may also gather data from our website's contact form, or when you voluntarily complete client surveys or provide information at meetings.

Why do we collect this data?

We process your personal data under the following lawful bases permitted by UK GDPR:

- Contract - to perform the services you have engaged us to provide. Without this information, we would be unable to fulfil our legal and regulatory obligations to you.
- Legal obligation - we are required to collect and retain certain data under FCA rules, anti-money laundering legislation, and other applicable law.
- Consent - for certain processing activities, such as marketing, where we will ask for your explicit consent in advance.
- Legitimate interests - where it is necessary for the purposes of our legitimate business interests, provided these are not overridden by your rights and interests.

If we need to collect special category data (e.g. health or medical conditions, trade union membership, or biometric identification data) we will obtain your explicit consent before doing so.

How will we collect your data?

We collect and record your data from a variety of sources, but rely mostly on information coming directly from you - usually across a series of meetings, beginning with our initial fact-finding meeting.

We may also collect data from third parties, such as credit reference agencies or identity verification services, where this is necessary to fulfil our legal or regulatory obligations.

How will we store your data?

All information you provide to us is stored securely. We hold copies of your data in both paper and electronic form, accessible only by current employees of the firm when providing advice or carrying out administrative tasks on your behalf.

Paper records

Paper files are kept in a secure location where unauthorised persons cannot access them:

- Files are locked in a drawer or filing cabinet with keys or access codes held securely by a limited number of authorised staff.
- When no longer required, paper files are shredded and treated as confidential waste.
- Employees ensure that paper documents and printouts are not left where unauthorised persons could see them.

Electronic records

Electronic data is protected against unauthorised access, accidental deletion, and malicious attack:

- Data is protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (such as USB drives or external hard drives), these are only used with approved, encrypted storage. When no longer required, such media is securely destroyed.
- Your data is backed up regularly, and backups are tested in line with our standard procedures.
- Data is not saved directly to personal laptops or mobile devices outside of our approved systems.
- All devices and systems containing personal data are protected by approved security software and a firewall.

Where data is transferred to or stored at a destination outside the United Kingdom (UK), we carry out appropriate due diligence to ensure the third party has sufficient safeguards in place to protect the security of your data. If adequate protections cannot be evidenced, we will not transfer data to that destination.

We take reasonable steps to protect your personal data in transit, but note that transmission of information via the internet cannot be guaranteed to be completely secure. We have procedures in place to detect and respond to any data breach, and all staff receive appropriate training.

Sharing your data

We will only share your personal data where data protection law permits it, and where appropriate safeguards are in place. We require all third-party service providers to keep your data secure and not to use it for their own purposes.

We do not sell or distribute your personal data to other organisations. Categories of third parties with whom we may share your data in the course of providing our services include:

- Identity verification providers - we use electronic identity verification services to fulfil our obligations under the Money Laundering Regulations. These providers check your details against relevant databases.
- Client relationship management and back-office systems - we use practice management software to record and manage client data securely.
- Investment platforms and product providers - we share relevant personal data with the platforms and product providers through which your financial arrangements are administered, and with investment managers appointed to manage your portfolio.
- Paraplanning services - where we engage third-party paraplanning support to assist in preparing financial planning reports, we share relevant client information with those firms under appropriate confidentiality and data processing terms.
- Marketing and newsletter services - where you have consented to receive marketing communications, we may use approved third-party providers to distribute newsletters on our behalf. These providers receive only the data necessary to deliver communications to you.
- Professional advisers - we may share information with your solicitor, accountant, or other professional advisers where you have asked us to liaise with them.
- Regulatory and legal authorities - we may be required to disclose personal data to the FCA, HMRC, the National Crime Agency, or other competent authorities where required by law.

Where we need to transfer your personal data to a destination outside the UK, we carry out appropriate due diligence to ensure that adequate protections are in place, in accordance with UK GDPR requirements.

Your rights

Under UK GDPR, you have the following rights in respect of your personal data:

- To be informed about the collection and use of your personal data.
- To request access to the personal data we hold about you (a Subject Access Request).
- To have inaccurate personal data rectified, or completed if it is incomplete.
- To request erasure of your personal data in certain circumstances.
- To request restriction or suppression of your personal data.
- To obtain and reuse your personal data across different services (data portability).
- To object to the processing of your personal data in certain circumstances.

To exercise any of these rights, please contact Ricky Chan at info@ifswp.co.uk or by post at: Thomas House, 84 Eccleston Square, Victoria, London, SW1V 1PX. We will respond within one calendar month.

Please note that some of these rights are subject to conditions and may be limited by our legal and regulatory obligations to retain data, as described below.

How long will we hold your data?

We will retain your personal data for as long as necessary to perform our services and to comply with our regulatory obligations. We take reasonable steps to keep your personal data accurate and up to date.

Our minimum regulatory retention periods are:

- Three years - mortgage business
- Three years - insurance business
- Five years - investment business
- Indefinitely - pension transfer and pension opt-out business

We reserve the right to hold data for longer than the minimum periods stated above where there is a legitimate reason to do so, such as an ongoing professional indemnity requirement or an unresolved complaint.

If our relationship ends, we will retain your personal data for a period of seven years after that date, unless a longer retention period is required by law, FCA regulation, or our professional indemnity insurer. Pension transfer and opt-out records are retained indefinitely as noted above.

Once the relevant retention period has expired, we will comply with any valid request for your data to be erased. Further details of our retention periods are available on request.

Can I access the data you hold on me?

Yes. You have the right to request a copy of the personal data we hold about you free of charge. Please contact Ricky Chan by email at info@ifswp.co.uk or by post at: Thomas House, 84 Eccleston Square, Victoria, London, SW1V 1PX.

We will provide the information within one calendar month of receiving your request. We reserve the right to charge a reasonable fee if a request is manifestly unfounded or excessive.

Marketing

As a client of the firm, we may occasionally send you marketing material to keep you informed of news and developments we believe may be of interest to you, or to provide information on other products and services. We will ask for your consent and your preferred method of contact before sending you anything.

You may withdraw your consent at any time by clicking the unsubscribe link in any marketing email, or by contacting Ricky Chan at info@ifswp.co.uk. We will not send you further marketing communications after receiving your request.

What if I am unhappy with how you have processed my data?

If you have a concern about the way we are collecting or using your personal data, please raise this with us in the first instance by contacting Ricky Chan at info@ifswp.co.uk or by post at: Thomas House, 84 Eccleston Square, Victoria, London, SW1V 1PX.

If you remain dissatisfied, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office

Website: https://ico.org.uk/make-a-complaint/

Telephone: 0303 123 1113

Post: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Review of this policy

We review this privacy policy at least annually and whenever there is a material change to our data processing activities. We reserve the right to update this policy at any time and will notify you of any changes that materially affect how we collect, store or process your personal data. The current version of this policy is available on request and on our website at www.ifswp.co.uk/privacy/