FUTURE FINANCIAL PLANNING

Privacy Policy

How we use and protect your personal information

Version 5.3 • 1 November 2026

FUTURE
FINANCIAL PLANNING

We use personal information to provide independent financial planning and regulated financial advice, support our clients and meet our legal and regulatory responsibilities. Our services include investments, pensions, retirement planning, income drawdown, annuities and related financial-planning matters. Technology helps us deliver these services; our advisers remain responsible for recommendations and suitability decisions.

This notice explains what we collect, how we use it and your choices. Please contact us if you would like it in larger print or another accessible format.

In this policy

1 Who we are

2 Who this notice covers

3 Information we collect

4 Where information comes from

5 Why we use information and our lawful bases

6 Health and other sensitive information

7 Meeting recording and transcription

8 Artificial intelligence and Microsoft 365

9 Our client portal and My Future app

10 Who receives information

11 Processing outside the United Kingdom

12 Security and retention

13 Your choices and rights

14 Marketing, cookies and app technologies

15 Privacy complaints

16 Updates to this notice

1 Who we are

Future Financial Planning Limited is the controller responsible for the personal information we use for our financial-planning business. We are registered in England and Wales under company number 09302385, authorised and regulated by the Financial Conduct Authority (FCA) under reference 716526, and registered with the Information Commissioner's Office (ICO) under reference ZA112997.

Contact	Details
Data Protection Lead	John Markham
Email	info@futurefp.com
Telephone	01255 377009
Post	Unit C, Swains Farm Buildings, 89 The Street, Little Clacton, Essex, CO16 9LT
Website	www.futurefp.com

2 Who this notice covers

This policy covers existing, prospective and former clients; website, client portal and My Future app users; and people connected to clients, including partners, dependants, beneficiaries, trustees, attorneys, executors and authorised representatives. It also covers professional connections, business and supplier contacts, service-provider contacts, and other people whose information is relevant to a client's financial planning. We may give additional information for a particular service or collection of information.

3 Information we collect

Identity and contact details

name, address, date of birth, contact details, nationality, National Insurance number and identity documents.

Personal circumstances

family and household circumstances, employment and business information, objectives, preferences, communication requirements and support needs, including vulnerability information.

Financial information

income, spending, tax, assets, liabilities, bank details, source of funds and wealth, and pension, investment, mortgage and insurance records.

Planning and advice records

attitude to risk, capacity for loss, knowledge and investment experience, cash-flow information and planning assumptions, recommendations, suitability assessments, instructions and transaction records.

Communications

correspondence, secure messages, uploaded documents, electronic signatures, document-delivery records, meeting recordings, transcripts, summaries, notes and actions.

Sensitive information

health and other special category information where relevant and lawfully processed, for example for insurance, retirement or financial planning, or to adapt our service to your support needs.

Financial-crime information

identity and screening results, sanctions and politically exposed person information, and criminal-offence or fraud information where necessary and legally permitted.

Service and technical information

account identifiers, IP addresses, device and sign-in information, security logs, app activity, notification settings and diagnostic information generated by the services you use.

4 Where information comes from

We obtain information from you through meetings, calls, forms, correspondence, our website, appointment-booking services where used, portal and app. We may also receive it from people authorised to act for you; product providers, platforms, pension schemes, insurers and investment managers; employers and professional advisers; and identity-checking, fraud-prevention and financial-crime screening services. Public registers and other publicly available sources may be used for relevant checks.

Connected investment services may provide holdings, valuations and other account information. Our technology suppliers process information generated when you use our services, including messages, uploaded documents and meeting transcripts.

Please give us information about other people only where relevant and make them aware of this notice where practicable. We also assess our own obligation to provide privacy information to them; asking you to pass on this notice does not replace that responsibility.

5 Why we use information and our lawful bases

UK data protection law requires a lawful basis for each use of personal information. The table sets out our principal purposes and bases. Where a record serves more than one purpose, the basis for each purpose applies separately.

Purpose	Lawful basis
Prepare and provide advice, implement agreed instructions and deliver our ongoing service.	Contract: necessary to perform our agreement with you, or take steps you request before an agreement.

Purpose	Lawful basis
Carry out applicable identity and anti-money-laundering checks; meet suitability, regulatory record-keeping and complaint-handling duties.	Legal obligation: compliance with applicable financial-services and financial-crime requirements.
Administer enquiries and business relationships, maintain service continuity, monitor service quality, secure systems and prevent misuse.	Legitimate interests in running, improving and protecting our business and supporting clients, where those interests are not overridden by your rights.
Record and transcribe meetings and prepare working notes, summaries and draft communications using approved technology.	Legitimate interests in accurate records, reliable follow-up, continuity of service and efficient administration, subject to necessity, proportionality and your right to object. Special category information also requires the Article 9 condition explained in sections 6 and 7.
Provide requested portal and app functions, including messages, documents, signatures and connected portfolio information.	Contract for delivery of the agreed service; legitimate interests for separate security, fraud-prevention and proportionate diagnostic activities.
Establish, exercise or defend legal claims.	Legitimate interests in protecting legal rights; legal obligation where a specific legal requirement applies.
Send optional marketing.	Consent where required. Where the electronic-marketing soft opt-in lawfully applies, legitimate interests in promoting relevant services, with an opportunity to opt out when details are collected and in each message.
Hold professional and supplier contact information.	Legitimate interests in obtaining services and managing business relationships; contract where the individual is personally a party to it.

> When relying on legitimate interests, we assess the purpose, necessity and effect on your rights. We do not treat agreeing to this notice, using the app or remaining a client as blanket consent to all processing.

6 Health and other sensitive information

Processing special category information requires both a lawful basis under Article 6 and an additional condition under Article 9 of the UK GDPR. Explicit consent is our chosen Article 9 condition for routine use of health and other special category information in financial planning and support where appropriate. We explain the information and purposes, including any recording or AI-assisted processing, so you can make a specific choice. Another documented Article 9 condition may apply to a particular purpose, as explained below.

> **We do not treat attendance, silence, acceptance of this notice or simply continuing with a meeting as explicit consent.** You may withdraw consent by contacting us, without affecting processing already carried out lawfully. **Declining or withdrawing consent to recording sensitive information does not prevent you accessing our advice service**; we will use manual notes or another appropriate method. Any continued use of sensitive information, including in manual notes, still requires an Article 6 basis and an Article 9 condition. We will explain if a particular service needs information that you do not wish us to process.

Where necessary to establish, exercise or defend legal claims, we may use relevant special category information under Article 9(2)(f). This is a separate, limited purpose, not a general basis for routine recording or AI use. We do not rely on FCA regulation alone as permission to process sensitive information.

If a different statutory condition is needed for a particular activity, we will identify it, meet its requirements and provide relevant privacy information before that activity, unless the law permits otherwise. Criminal-offence information is subject to separate legal restrictions; we use it only where authorised by law with the required safeguards.

7 Meeting recording and transcription

We normally use approved technology to record client meetings and prepare transcripts, draft notes and actions. We give all attendees clear information about recording and its purposes before recording begins, for example through onboarding documents, meeting confirmations or a notice at the start of the meeting. We draw your attention to this information and explain how to raise concerns. A recording may capture information about finances, health and other people. We seek to avoid collecting information that is not needed.

Routine recording is based on legitimate interests in accurate records, reliable follow-up, continuity of service and efficient administration, as described in section 5. Where a meeting may include health or other special category information, we ask for your explicit agreement to that information being captured in the recording and processed to produce a transcript and meeting record. We may obtain this specific consent in advance where it covers the information and processing involved and remains valid. This is separate from the Article 6 basis for routine recording. You may decline without losing access to our advice service, in which case we use manual notes or another appropriate method for that information. If sensitive information arises unexpectedly and the relevant agreement is not in place, we will pause the recording where practicable and agree how to continue. We will restrict further use of any sensitive material already captured and arrange its deletion or redaction unless a documented lawful basis and Article 9 condition justify retaining it.

You can object to recording before or during a meeting. We will consider your circumstances and stop the processing unless we can demonstrate compelling legitimate grounds overriding your interests, rights and freedoms, or the processing is necessary for legal claims. We will explain our response and consider alternatives, such as manual notes. **An objection to recording does not, by itself, prevent you receiving advice.**

AI transcripts and summaries can contain mistakes. We check material content before relying on it in advice or treating it as the final client record. You can ask us to correct inaccurate personal information. Access is limited to people and service providers who need it for the relevant purpose.

8 Artificial intelligence and Microsoft 365

We use Microsoft 365 for business communications, documents, collaboration and storage. Approved business AI tools, including Marloo and Microsoft 365 Copilot where enabled, may assist with transcription, summaries, administration, finding relevant business information, and drafting meeting notes, actions, correspondence and advice-related documents.

These tools may process relevant meeting content, documents, communications and client-record information made available to them. We limit their use to approved business purposes and authorised access. AI may help identify matters for an adviser to consider, including possible support needs, but an adviser assesses the context and decides what action is appropriate.

AI does not replace professional judgement. An authorised member of our team with appropriate knowledge and competence reviews material outputs before use. **Our advisers remain responsible for recommendations and suitability assessments.** We do not make decisions about you with legal or similarly significant effects solely by automated means.

Client information must not be entered into unapproved public or consumer AI services. Before authorising AI processing, we assess the purposes, information involved, access, supplier terms, model-training permissions, security, retention and onward processing. The information made available to an approved tool is limited to its authorised purpose.

We assess new AI services and material changes before use. If a change introduces a new purpose or materially changes how your information is used or shared, we update the relevant privacy information and obtain any consent required.

9 Our client portal and My Future app

We use Plannr for client relationship management and our client portal. The My Future app uses Plannr software. Where made available to you, the app supports our financial-planning service. We remain responsible for our use of your client information. Where Plannr processes that information on our behalf, it does so under the applicable processing arrangements.

Depending on the services available to your account, the portal and app may provide secure messaging, document upload and download, electronic signatures, push and service notifications, and information from connected investment platforms, including portfolio holdings and valuations. Connected information depends on the relevant provider and may not be current in real time.

To provide and protect the service, relevant account details, messages, documents, signature records, connection information, device identifiers, sign-in records, security events, notification information and diagnostics may be processed. Device permissions and optional features are explained when requested. You can manage available permissions and notifications through the app or device settings; disabling them may affect the relevant feature.

Where device-based biometric sign-in is offered, the device's security functions are used to authenticate access. The information processed and available choices are explained when the feature is enabled. Please also consult your device provider's privacy information.

The app is not currently used for bank-account transaction feeds. If we introduce that functionality, we will explain the data use and relevant permissions before you connect an account.

Apple, Google and any independent service you choose to use may process information for their own purposes under their own notices. Please protect your sign-in details and contact us promptly if you suspect unauthorised access.

10 Who receives information

We share information where needed for the relevant service or lawful purpose. Recipients can include:

- Product providers, platforms, pension schemes, insurers, investment managers, custodians and administrators.
- Representatives and professional advisers involved in your affairs, where authorised or otherwise lawfully permitted.
- External paraplanners, compliance consultants, accountants, auditors, legal advisers, professional indemnity insurance brokers and insurers, where disclosure is necessary for their relevant work or a legal obligation.
- Technology and support suppliers, including Plannr, Marloo and Microsoft, and providers of fact-finding, attitude-to-risk assessment, cash-flow modelling, investment research and analysis, suitability-report preparation, hosting, communications, appointment booking, electronic signatures, identity checks, cybersecurity, device management and backups.
- Identity-checking, fraud-prevention and financial-crime screening organisations.
- The FCA, ICO, HMRC, Financial Ombudsman Service, Financial Services Compensation Scheme, courts and other competent authorities, where required or lawfully permitted.
- A prospective purchaser, successor or continuity provider where necessary for a genuine business transfer, succession or wind-down, with proportionate disclosure and appropriate confidentiality safeguards.

We do not sell your personal information. Suppliers acting as processors must operate under appropriate data-processing contracts and our documented instructions. Some recipients, such as product providers and regulators, act as independent controllers and have their own privacy notices. A supplier may also be a controller for separate activities, such as managing its own business relationship; its role depends on the processing involved.

11 Processing outside the United Kingdom

Our suppliers and their authorised subcontractors may store or access information outside the UK. Where this is a restricted international transfer, we use a lawful transfer route: applicable UK adequacy regulations or appropriate safeguards, such as the UK International Data Transfer Agreement or the UK Addendum to the European Commission's Standard Contractual Clauses. We assess the protection required for the transfer and put additional measures in place where necessary.

Contact our Data Protection Lead for information about the destinations and safeguards relevant to your information, including how to obtain a copy of applicable safeguards, with confidential details redacted where appropriate.

12 Security and retention

We are responsible for using technical and organisational measures appropriate to the risks to your information and for requiring appropriate safeguards from suppliers handling it on our behalf. No technology can guarantee complete security. We investigate suspected breaches and notify affected people and authorities where legally required.

We keep information for the period needed for its purpose, taking account of the type of advice, applicable rules, contractual commitments, complaints and legal claims. Closing an app account or ending our relationship does not automatically remove records we must or are otherwise lawfully entitled to retain.

Record	Retention approach
Final advice and suitability records	Certain pension transfer, conversion, opt-out and free-standing additional voluntary contribution (FSAVC) suitability records are retained indefinitely. Relevant life-policy and pension suitability records are generally retained for at least five years, and other suitability records covered by the applicable rule for at least three years. Other legal and regulatory requirements may prescribe different periods. Records are kept longer only where justified.
Anti-money-laundering records	Generally five years after the end of the business relationship or completion of the relevant occasional transaction, subject to applicable legal exceptions and deletion requirements.
Raw recordings, transcripts and intermediate AI drafts	Reviewed after the final record is completed and checked. Raw audio, transcripts and intermediate AI drafts are retained only while needed for verification, outstanding actions, complaints, claims or another documented purpose; they are not automatically kept for the full advice-file period. Where a recording or transcript is itself a required regulatory record, we retain it for the applicable regulatory period.
App, security and diagnostic records	Kept for the period needed to operate and protect the service, investigate incidents and resolve relevant issues, considering the type of log and supplier settings.

Record	Retention approach
Marketing preferences and suppression records	Kept as needed to administer your choice and avoid contacting you contrary to an opt-out.

A complaint, investigation, legal claim or preservation requirement may justify longer retention of relevant records. We restrict access and use where appropriate. When retention is no longer justified, information is securely deleted or anonymised, including through the applicable backup lifecycle. You can ask us for the period or criteria applying to a particular record.

13 Your choices and rights

Some information is needed to fulfil our agreement or meet legal requirements, including identity checks and assessing the suitability of advice. If you do not provide necessary information, we may be unable to start or continue the relevant service or carry out an instruction. We will explain what is needed and why. Optional permissions and marketing choices are treated separately.

- ✓ You can request access to your personal information and ask us to correct inaccuracies.
- ✓ You can request erasure, restriction or a portable copy where the relevant legal conditions apply.
- ✓ You can withdraw consent at any time for processing based on consent, without affecting its previous lawful use.
- ✓ You have safeguards in relation to significant decisions made solely by automated processing. As explained in section 8, we do not make such decisions about you.

Your right to object

> **You can object at any time to direct marketing, and we will stop using your information for that purpose.** You can also object, for reasons relating to your circumstances, to processing based on legitimate interests, including meeting recording. We must stop that processing unless we demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or need it for legal claims. You can object verbally or in writing using the contact details in section 1.

Other rights are subject to legal conditions and exemptions. For example, required regulatory records may not be eligible for deletion. We will explain any refusal or limitation and your complaint options. We may request proportionate identity checks. Requests are normally answered within one month; where the law permits extra time or a pause, we will explain this and keep you informed. **Requests are normally free of charge.**

14 Marketing, cookies and app technologies

You can unsubscribe from marketing using the option in the message or by contacting us. Essential service, security and regulatory communications may still be sent; we do not treat those as permission to send marketing.

Our website and app may use cookies, local storage, software development kits and similar technologies to store or access information on your device. Their use can include service functions, security and, where enabled, analytics or advertising. Relevant booking tools and integrations may also use these technologies. The applicable cookie or app information explains the technologies in use, their purposes, providers, duration and your choices.

We seek consent before using technologies that require it. Where a legal exception applies, we meet its conditions, including any requirement to give information and an easy way to object. You can change the available choices through the relevant controls. Device permissions and app notifications can also be managed in the app or device settings; these permissions do not by themselves provide consent for unrelated tracking or marketing.

15 Privacy complaints

If you are concerned about how we handle your information, contact our Data Protection Lead using the email, telephone number or postal address in section 1. You do not need to use a particular form. Please describe your concern and how you would like us to contact you.

We will acknowledge your complaint promptly and in any event within 30 days. We will make appropriate enquiries without undue delay, keep you informed of progress and tell you the outcome without undue delay. We will explain any action taken and any further steps available to you.

> **You also have the right to complain to the ICO.** Information is available at https://ico.org.uk/make-a-complaint/ or by telephone on 0303 123 1113. The ICO's postal address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. This does not affect any separate right to complain about our financial advice or service.

16 Updates to this notice

We review this notice when our services, technology or legal obligations change. The current approved version will be available on our website and through the app. We bring material changes to your attention where appropriate and provide information about new purposes before processing begins, unless the law permits otherwise.