

MERCURY
WEALTH MANAGEMENT

Privacy Policy

Version 3.4 | 28 October 2026

01642 670307

clientservices@mercurywealth.co.uk

About this policy

This policy explains how we collect, use, share and protect personal information when you enquire about or use our financial planning and wealth management services. It also explains how we use technology to support our work, how we record meetings, and your choices and rights.

We handle personal information in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 and other applicable data protection law, as amended.

Who we are
Mercury Wealth Management Limited is the controller of the personal information described in this policy. This means we are responsible for deciding why and how it is used.

Our address is Mercury House, 1 Massey Road, Teesdale Business Park, Stockton-on-Tees, TS17 6DY. For questions about your information or to exercise your rights, contact Oliver Bourke at dataprotection@mercurywealth.co.uk or write to us at this address.

Mercury Wealth Management Limited is registered in England under company number 4981483 and is authorised and regulated by the Financial Conduct Authority under reference 455415.

The information we collect

We collect information relevant to our services, including:

• identity and contact details, verification records, residential address, countries of tax residence and relevant tax identification numbers;
• information about your family, dependants and other people relevant to your financial planning;
• your financial circumstances, including income, expenditure, assets, liabilities, pensions, investments and insurance;
• your objectives, priorities, preferences and attitude to investment risk;
• correspondence, instructions, documents and records of our work with you;
• information about your health or other sensitive circumstances where relevant to the service; and
• call and meeting participant details, recordings, transcripts, summaries and agreed actions, as explained below.

When we use technology to work with your information, relevant instructions entered into the system and the resulting responses or draft documents may also contain personal information.

We usually obtain information directly from you during meetings or through calls, correspondence, forms and our client portal. Where you have authorised this, we also obtain information from your professional advisers and organisations holding your existing pensions, investments or insurance. We may obtain identity-check information from verification services where needed to meet our legal obligations.

Please tell us if your circumstances change or information we hold is inaccurate. If you give us information about another person, please make them aware of this policy where appropriate. We remain responsible for providing them with privacy information where required.

How and why we use your information

We use information to understand your needs, assess suitability, check service and provider eligibility, implement authorised instructions and administer our relationship. This includes checking tax-residency declarations and meeting relevant provider, legal and regulatory requirements. We also use information for staff training, service monitoring, queries, complaints and fraud prevention.

The lawful basis depends on the purpose:

• Providing our services. We use information where necessary to perform our contract with you or take steps at your request before entering into a contract. This includes understanding your needs, preparing advice and administering agreed services.
• Meeting legal obligations. We use and retain information where required by law, including relevant financial-services record-keeping and financial-crime prevention obligations.
• Our legitimate interests. Where necessary and proportionate, we use information to maintain accurate records, train our staff, monitor service quality, manage and improve our services, maintain security, respond to complaints and establish or defend legal claims. This includes the recording, transcription and summarisation described below. We assess each purpose and balance our interests against your rights, including whether less intrusive methods can meet the need. You can object, as explained under Your right to object.
• Your consent. We rely on consent where we specifically ask you to agree to a use of your information. You can withdraw that consent by contacting us. For ordinary recording, we rely on legitimate interests as explained below.

Where we need health information or other special-category information for our routine planning services, or recording would capture such information, we obtain your explicit consent where that is the applicable condition. These categories have additional legal protection. Where another permitted condition applies, for example where information is necessary for a legal claim, we explain the relevant basis as appropriate.

If you choose not to provide information that is necessary for our services or required by law, we may be unable to provide some or all of the service. We will explain the information needed and the effect of not providing it. Optional meeting recording is addressed separately below.

We seek your agreement where required before sending marketing communications. You can ask us to stop marketing to you at any time. We do not share your information with other organisations for their own marketing.

How we use technology

We use technology, including artificial intelligence, to support the administration and delivery of our services. This can help our team organise information, prepare draft documents and correspondence, support technical and regulatory research, and create meeting transcripts, summaries, file notes and action points. For general technical or regulatory research, we use material that does not identify clients. Where research concerns your particular circumstances, we use only information relevant to the task through approved services.

We use Microsoft business services, including Microsoft 365 Copilot. Where enabled, these services may use models developed by OpenAI or Anthropic, including Claude. The models and features available to us may change over time.

We also use specialist applications for functions such as meeting recording, transcription, summarisation, document preparation and business administration. We review applications before approving them for use with personal information, including their purpose, access arrangements, security and data protection terms.

Depending on the service and model used, information may be processed by Microsoft, a model provider or another service provider. Accessing a service through Microsoft does not necessarily mean that all processing takes place within Microsoft's systems or within the UK. The sharing and international-processing sections below explain this further.

We use information relevant to the task and restrict access to authorised users. Technology supports our people, who remain responsible for checking the work. We review technology-assisted outputs before relying on them in providing your service or sharing them with you.

Financial advice and recommendations are reviewed, approved and delivered by an appropriately qualified and authorised person. We do not use these tools to provide automated regulated financial advice directly to you, or to make decisions based solely on automated processing that have legal or similarly significant effects on you.

Using technology does not reduce our responsibility to exercise reasonable skill, care and diligence in providing our services.

Recording and transcribing meetings

We may record and transcribe meetings to keep an accurate record of our discussions, prepare file notes and identify agreed actions. Calls may also be recorded for staff training and monitoring purposes, including checking service quality and compliance with our procedures. We explain the purposes that apply before recording starts. Training in this section means training our staff.

We use meeting software and specialist recording, transcription and summarisation applications. Depending on the communication and the features enabled, we may capture your name, voice, video, shared content and the personal or financial information discussed. Transcripts, summaries and action points may also contain personal information.

How we tell you about recording

For planned meetings, we let you know in advance by email that the meeting is intended to be recorded and transcribed and explain how to ask us not to record. We display signs in meeting rooms where recording takes place. In video meetings, you can see a visible notification when recording is active. We also give a verbal reminder, including to people joining by telephone or joining late.

For telephone calls, we give a recorded announcement or tell you about recording and its purposes before it starts. Notices and reminders are intended to make the arrangements clear to everyone taking part.

Your choice and stopping recording

Where our assessment supports recording as necessary and proportionate, we rely on our legitimate interests in maintaining accurate records, training our staff and monitoring service quality. After we have explained the arrangements, we may record and transcribe unless you ask us not to. You can tell us in advance or at any time during the meeting or call.

If you ask us to stop, we will stop recording and transcription immediately. We can continue an ordinary client meeting using manual notes. If a particular communication must be recorded by law, we will pause or end that communication and explain any available alternative arrangements. We do not continue a communication unrecorded where the law requires a recording.

Sensitive information and staff training

Attendance, a room sign or a recording notification does not provide explicit consent to record health information or other special-category information. We obtain the required explicit consent before recording such information, or establish another applicable legal condition. If neither is available, we pause recording before the sensitive discussion and agree an appropriate way to proceed.

We select only the material needed for staff training or quality monitoring, restrict access and remove unnecessary identifying details. We use anonymised examples where these achieve the training purpose. Identifiable health or other special-category information is not reused for staff training without a separately established lawful basis and applicable special-category condition.

Copies and corrections

You can request copies of transcripts we hold of your calls or meetings by telling your Mercury contact or emailing dataprotection@mercurywealth.co.uk. We provide copies securely, subject to necessary lawful redactions or restrictions, including protection of other people's personal information. We explain any restriction. Our response arrangements are set out under Your rights.

Automated transcripts and summaries can contain mistakes. Our team checks the records used in providing your service. Please tell us if you believe a record is inaccurate, so that we can review it and correct it where appropriate.



Who we share information with

We share relevant information where needed for the purposes described in this policy. Recipients may include:

• insurance, pension and annuity providers, investment providers and platforms, investment managers, lenders and third-party administrators;
• providers of pension transfer comparison reports and other specialist analysis needed for your advice;
• your professional advisers, where you have authorised us to work with them;
• retained compliance consultants, auditors, legal and accounting advisers, and insurers where relevant to reviewing our work, managing risk or dealing with a complaint or claim;
• providers of identity verification and financial-crime prevention services;
• providers of cloud storage, business software, communications, document management and client portals, including Microsoft;
• specialist providers of meeting recording, transcription and summaries, and providers of AI models or services supporting the activities described above; and
• regulators, courts, law-enforcement bodies and other organisations where disclosure is legally required or otherwise lawfully necessary.

Our client portal, Mercury Insight, is provided and operated on our behalf by Moneyinfo Limited. We identify the product and service providers we recommend to you in our advice and supporting documents. Operational service providers may also process information before a recommendation is made, for example when hosting a meeting or helping us prepare its notes.

Processors acting for us must meet contractual duties for confidentiality, security and our instructions. Product providers and regulators may be independent controllers with their own privacy notices. Providers may use tax-residency details for reporting duties, including to HMRC.

We limit disclosures to information relevant to the purpose. Please contact us if you would like more information about the categories of organisations handling your information or the services involved.

Processing information outside the UK

We use, and may introduce from time to time, applications and service providers that store or otherwise process personal information outside the UK. This can include cloud services, meeting recording and transcription applications, and AI services. Processing outside the UK may include storage, technical support, transcription and the generation of summaries or other outputs, including processing in the United States.

Where a transfer is subject to UK international-transfer rules, we ensure that an appropriate legal mechanism is in place. Depending on the arrangement, this may be UK adequacy regulations recognising the relevant destination or recipient, or appropriate contractual safeguards such as the UK International Data Transfer Agreement or the UK Addendum to approved standard contractual clauses. Where required, we assess the protection in the destination and apply additional measures.

We assess new providers and changes to existing services before using them to process your information. If a material change affects how your information is used or protected, we update the relevant privacy information and obtain further consent where required.

You can contact dataprotection@mercurywealth.co.uk for information about relevant processing locations and the safeguards that apply to your information, including how to obtain a copy of those safeguards.

How we protect information

We use appropriate technical and organisational measures to protect personal information against unauthorised access, loss or misuse. These include access restrictions, confidentiality requirements, secure storage and appropriate protection when information is transferred.

Please keep passwords and access codes confidential and tell us promptly if you suspect that someone has gained unauthorised access to your account or information. No method of internet transmission is completely secure, but we take reasonable steps to protect information in transit and when held by us or our service providers.

How long we keep information

We keep personal information only for as long as it is needed for the purpose for which it was collected, or for another lawful purpose. The period depends on the type of information, the service provided, relevant legal and regulatory record-keeping duties, and the need to address complaints or legal claims.

We consider recordings, training material, transcripts, draft summaries and approved client-file records separately:

- Recordings used to prepare meeting notes are kept until the client record has been prepared and checked. We retain them beyond that point only where necessary for an identified client matter, complaint, legal claim or applicable record-keeping requirement. We record the reason for extended retention and set a review date. Material selected for staff training or quality monitoring is addressed separately below.
- Staff training and quality-monitoring material is limited to the relevant content and kept only for the associated training or review purpose. We set a retention period and review date for the material selected. It is then deleted or anonymised unless a separate, documented retention requirement applies. Source call recordings awaiting review or selection follow a defined retention period. Recordings not selected are deleted when that period ends, unless a separate, documented retention requirement applies.
- Transcripts and draft summaries are kept while needed to prepare and verify the client record. We retain them beyond that point only where they remain necessary for our services, record-keeping duties or a complaint or claim.
- Approved file notes, advice and supporting records are kept for the period needed to provide our services, meet the requirements applying to the work undertaken and address relevant complaints or claims. This may extend beyond the end of our relationship.
- Technology interaction records containing personal information, including relevant instructions and generated responses, are subject to retention arrangements appropriate to their content and purpose. Material that forms part of the client record is retained with that record where appropriate.

We review the continuing need for information and delete or anonymise it when it is no longer required. Deletion arrangements take account of copies held in service-provider systems, exports and backups. Where a legal hold or retention requirement applies, information may remain protected from deletion and its use is restricted to the relevant purpose.

You can ask us for further information about the retention period or criteria applying to a particular record.

Your rights

Depending on the circumstances and the lawful basis for processing, you may ask us to:

• provide access to a copy of your personal information;
• correct inaccurate information or complete information that is incomplete;
• delete information where there is no lawful reason to continue keeping it;
• restrict how we use information in circumstances provided for by law; and
• provide information you have given us in a commonly used electronic format, or transfer it to another organisation, where the conditions for data portability are met.

Your right to object

You can object to processing based on legitimate interests for reasons relating to your particular situation. We will consider your objection and explain the outcome. You have an unconditional right to object to the use of your personal information for direct marketing.

Withdrawing consent and making a request

Where we rely on consent, you can withdraw it at any time by telling your Mercury contact or contacting dataprotection@mercurywealth.co.uk. Withdrawal does not affect processing carried out lawfully before consent was withdrawn. It does not automatically require deletion of necessary client-service records retained on another lawful basis. We explain that basis if it applies to your request.

You can make a request verbally or in writing. We respond without undue delay and normally within one month, subject to any lawful extension or pause to the time limit. We explain any extension or pause and what it means for your request. We do not normally charge. We may need to confirm your identity and will explain any lawful restriction or exception that affects our response. In particular, a deletion request may not cover information we must retain to meet a legal obligation or establish, exercise or defend a legal claim.

Questions and complaints
Please contact Oliver Bourke at dataprotection@mercurywealth.co.uk or write to us at Mercury House, 1 Massey Road, Teesdale Business Park, Stockton-on-Tees, TS17 6DY.

You can also complain to the Information Commissioner's Office at ico.org.uk/make-a-complaint, by telephone on 0303 123 1113, or by post to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Changes to this policy
We review this policy and update it when necessary. The current approved version is available in the disclosure section of our website. We will bring material changes to your attention where appropriate and provide any additional information required before using your information for a new purpose.



www.mercurywealth.co.uk

01642 670307

clientservices@mercurywealth.co.uk

Mercury House, 1 Massey Road
Teesdale Business Park
Stockton-on-Tees
TS17 6DY

CISI CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT CHARTERED FIRM™

CISI CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT ACCREDITED FINANCIAL PLANNING FIRM™

Mercury Wealth Management is authorised and regulated by the Financial Conduct Authority (FCA). Reference number: 455415
Company Registration Number: 4981483