Privacy notice

Website, client portal and professional services

This notice explains how Parkwood Louvigny Limited collects and uses personal information through our website, client portal and accountancy practice. It covers enquiries, onboarding, professional services and our administration of those services.

It applies to clients and prospective clients; directors, partners, beneficial owners and authorised contacts; and other people whose information we receive through our work, including employees, customers, suppliers and relevant family members.

This notice provides information, not a request for blanket consent. Signing an engagement, acknowledging this notice or using the portal does not give permission for every possible use of your information.

Contact	Details
Data controller	Parkwood Louvigny Limited | Company number 12324814
Privacy contact	James Bodycombe
Email	jbodycombe@parkwoodlouvigny.co.uk
Telephone	07466 921648
Postal address	Hectors House, Pankhurst Close, Exmouth, Devon EX8 2RN
ICO registration	ZC273812

1. Our responsibility for your information

We are the controller when we decide why and how information is used for our professional work, client acceptance, anti-money laundering checks, practice administration and legal obligations. We remain responsible for that processing when a service provider handles information on our behalf.

For particular tasks carried out solely on a client's documented instructions, such as an agreed payroll processing service, we may instead act as that client's processor. The client is then responsible for its controller obligations and its own privacy information. Our role depends on the actual task, not simply the name of the service. We can explain which role applies to your information.

This notice concerns the limited company. It also applies to records that have been lawfully transferred to it from a predecessor practice; it does not retrospectively change who was responsible for earlier processing.

2. Information we collect and where it comes from

Information	Examples and sources
Identity, contact and authority	Names, addresses, contact details, dates of birth, identity documents, signatures, roles and authority to instruct us. Usually supplied by you, your organisation or an authorised representative.
Business and financial records	Ownership and control, business activities, transactions, accounts, bank information, invoices, receipts, assets, income and expenses. Supplied by clients, authorised contacts and accounting or document systems.
Tax and payroll information	Tax references, National Insurance numbers, tax residence, employment, pay, deductions, benefits and pension information. Where relevant, information about dependants or family circumstances needed for the agreed work.
Due diligence and screening	Identity and address checks, beneficial ownership, source of funds or wealth where necessary, sanctions and politically exposed person screening, relevant adverse media and documented risk decisions.
Communications and service records	Enquiries, correspondence, meetings, professional enquiries, instructions, agreed terms, work papers, approvals, submissions, receipts and complaints.
Portal and technical records	Login and verification events, account identifiers, document access and signing events, timestamps, browser/device information, IP addresses or hashed IP records, and security or delivery logs.
Website use	Pages visited, referral information, approximate location, device/browser information and interactions, where the relevant optional analytics are enabled. Section 10 explains cookies and choices.

We may also obtain relevant information from HMRC, Companies House, other public registers, the UK Sanctions List, professional advisers, previous accountants with appropriate authority, and identity or screening providers. Publicly available information is still personal information and is used only for a relevant purpose.

If you give us information about someone else, you must have a lawful reason to do so and should make this notice available to them. We remain responsible for our own transparency duties. Where we obtain information indirectly, we provide appropriate information within the applicable period, normally no later than one month, or earlier at first communication or disclosure, unless a lawful exception applies.

We collect only information relevant to the task. Please do not send passwords, one-time codes, identity documents, bank details or sensitive records through the basic website enquiry form or public social-media messages. Contact us to arrange an appropriate document-sharing route.

3. Why we use information and our lawful bases

The UK GDPR requires a lawful basis for each purpose. More than one basis may apply to different uses of the same record; we do not treat consent as a substitute for a legal duty.

Purpose	Basis and explanation
Responding to enquiries and agreeing work	Contract: steps you ask us to take before entering a contract with you as an individual. Legitimate interests: responding to business enquiries and dealing with people representing organisations.
Providing agreed accountancy, bookkeeping, tax, VAT, payroll and related services	Contract where you are personally our client. Legitimate interests in providing the agreed professional service where the client is an organisation or the information concerns another person. Legal obligation where a specific obligation applies to us. Processor tasks follow the client's lawful documented instructions.
Client acceptance, identity checks, AML, sanctions and required disclosures	Legal obligation where required by applicable money laundering, sanctions or other legislation. Legitimate interests for proportionate checks to prevent fraud or protect the practice where there is no specific legal duty. Sensitive information requires an additional condition, explained in section 5.
Running the practice and protecting records	Legitimate interests in secure administration, access control, quality assurance, accurate records, resolving complaints, collecting fees and establishing or defending legal claims. Legal obligation for our own statutory records and required responses to authorities.
Professional monitoring and regulatory cooperation	Legal obligation where imposed by law. Otherwise legitimate interests in meeting professional standards, cooperating with lawful practice reviews and maintaining the quality of services, subject to confidentiality and individual rights.
Optional analytics and relevant marketing	Consent for the optional website analytics described in section 10. Marketing consent where required by electronic marketing rules; otherwise the limited legitimate interests described in section 11.

Where we rely on legitimate interests, we consider whether the use is necessary and whether your interests, rights or freedoms override it. Our interests do not give us unrestricted permission to use personal information.

Your right to object: you may object to processing based on legitimate interests for reasons connected with your situation. You may object to direct marketing at any time, without giving a reason. Contact James Bodycombe using the details at the start of this notice.

Some information is required by law, or is necessary to agree and deliver the service. Without adequate identity checks, authority or relevant records, we may be unable to accept an engagement, complete particular work or make an authorised submission. Refusing optional marketing or website analytics does not prevent you from becoming a client.

4. Anti-money laundering and identity checks

We use Firmcheck and the identity or screening providers used for the relevant check to help verify identity, understand ownership and control, assess risk and meet applicable duties. Checks may compare information with identity, address, company, sanctions, politically exposed person and adverse-media sources. We review relevant results and investigate material inconsistencies; a possible match is not automatically treated as an adverse finding.

Personal information obtained for the purposes of the Money Laundering Regulations is used only to prevent money laundering or terrorist financing unless another use is permitted by law or you separately consent to it. It is not automatically available for marketing, unrelated analytics or general AI training.

We may have to make a report or disclose information to an appropriate authority. The law can restrict what we may tell you about such a report or investigation. These restrictions do not remove our other data protection responsibilities.

Electronic checks can include a photograph, document-chip checks, liveness checks or face matching. A photograph is not automatically special-category biometric information; biometric processing used to identify a person uniquely has additional legal requirements. Section 5 explains our approach.

5. Sensitive, biometric and criminal-offence information

We do not need sensitive information for every engagement. Where the agreed work requires it, records may include health information, trade-union deductions or other special-category information. Screening may also reveal sensitive information or information about alleged offences, convictions or related proceedings.

In addition to an ordinary lawful basis, we require a relevant special-category condition. This may be employment and social protection law for appropriate payroll information, establishing or defending legal claims, or a substantial-public-interest condition in UK law for necessary regulatory or crime-prevention work. The conditions and any required safeguards must apply to the particular use. For other service-related sensitive information, we seek explicit consent where appropriate or do not collect it. Where we are only a processor, we act under the controller's lawful instructions.

For biometric identity verification based on consent, we ask for a separate, explicit and informed choice before the biometric check. The check-specific information identifies the provider and explains the data, purpose and retention. Acknowledging this notice is not that consent. You can withdraw consent to further consent-based biometric processing and ask about a suitable non-biometric way of completing the required identity checks. We still need to complete lawful due diligence before accepting or continuing the work.

Criminal-offence information is handled only where UK law authorises the relevant processing and its safeguards are met, for example for applicable regulatory requirements, preventing or detecting unlawful acts, or legal claims. We do not assume that an ordinary legitimate interest alone permits this processing.

6. Who receives information

We share relevant information only for the purposes described in this notice and with an appropriate legal basis, authority and confidentiality arrangements. Recipients can include:

- HMRC, Companies House and other authorities or bodies to which an authorised filing, report or response is made. Information filed on a public register may become publicly available under that register's rules.
- Your authorised contacts and advisers, a previous or successor accountant where appropriate, and other people involved in the agreed work. We do not assume that every director, employee or family member may see every personal record.
- AAT, its appointed practice reviewers, other lawful regulators, courts and law-enforcement bodies where a relevant duty or properly justified disclosure applies.

- Professional advisers, insurers and suitably appointed support providers where necessary for advice, quality review, a complaint, a claim or a lawful continuity arrangement.
- The technology providers below, to the extent required for the relevant service.

Provider or service	Relevant use
Xero and Hubdoc	Accounting, bookkeeping, payroll where used, and collection or extraction of accounting documents.
Firmcheck and its relevant verification providers	AML records, identity verification, screening and risk-management workflows. The providers used for an individual identity check are identified in its check-specific information.
Google Workspace, Microsoft Outlook and Dropbox	Business communications, calendars, documents, file storage and authorised sharing.
Vercel, Supabase and Resend	Website and portal hosting; portal authentication, database and document storage; transactional emails, which may include copies of engagement documents.
Web3Forms (Web3Creative)	Delivery and processing of public website enquiries, including related security and spam checks.
Google Analytics 4 and Microsoft Clarity	Optional public website usage statistics and interaction/session analysis, subject to the choices in section 10.
Make and OpenAI-based tools, where used for the task	Controlled administrative automation, document handling and assisted analysis or drafting, subject to section 8.
Communication or referral platforms you use to contact us	The relevant platform processes messages and account information under its own terms; we use the information received to respond and manage the enquiry.

Not every provider receives every client's information or a complete client file. Suppliers may use subprocessors under their service arrangements. Some recipients, including regulators and providers acting for their own account administration or legal duties, are separate controllers. You can ask us which providers are relevant to your information and for further details of their role.

We do not sell client information. If the practice is transferred or a continuity provider needs access, any necessary disclosure will be subject to a lawful basis, suitable confidentiality safeguards and appropriate information to affected people. This notice is not itself permission for an unrestricted transfer of client files.

7. International processing

Some of our providers and their support or subprocessors operate outside the UK. Information may therefore be stored or accessed in other countries, including the European Economic Area, the United States, New Zealand and India. A database located in the UK does not mean that all support, communications or related processing stays in the UK.

For a restricted transfer, we require a lawful UK transfer mechanism. This may be UK adequacy regulations for the particular destination and recipient, or appropriate contractual safeguards such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with the required assessment and any additional measures. We do not assume that every US recipient is covered by the UK-US Data Bridge.

Web3Forms operates from India and uses infrastructure in multiple regions. Its published data processing terms include Standard Contractual Clauses and the UK Addendum for relevant transfers. Firmcheck also identifies overseas group or subprocessor involvement. Other providers' arrangements depend on the product and service used.

Contact us to ask where your information is processed, which transfer mechanism applies, and how to obtain a copy or description of the relevant safeguards, with confidential material redacted where necessary.

8. Automation and artificial intelligence

We use software to organise records and support our work. Depending on the task, automation or AI may extract information from documents, suggest classifications, flag inconsistencies or assist with administration, analysis and drafting. This may involve features within our service providers as well as separately approved tools.

Our approach is to use only the information needed for the task, remove identifying details where practicable, restrict access and use appropriate supplier terms and settings. We do not authorise identifiable client information to be used for general-purpose AI model training. A tool's subscription name alone is not an assurance about its data use.

James Bodycombe remains responsible for client acceptance, professional judgements and approval of work. We do not make decisions about you with legal or similarly significant effects based solely on automated processing. A software flag is subject to human consideration, and you can ask us to review a relevant result or correct inaccurate information.

Automated tools do not give authority to submit a tax return, sign an agreement, make a payment or disclose information beyond the agreed purpose. Any materially different future use would require an appropriate assessment, lawful basis and further information before it begins.

9. How long we keep information

We retain information for a defined purpose, not indefinitely because storage is available. Different records have different periods. We keep only what remains necessary, and delete, return or anonymise information when the relevant period and any justified hold end.

Record	Retention period or decision rule
Enquiries which do not become engagements	Our ordinary enquiry correspondence is retained for up to 12 months after the last meaningful contact, unless a complaint, legal duty or another specifically justified purpose requires longer. If you become a client, relevant information moves into the applicable client record category.

Record	Retention period or decision rule
Website form delivery copies	Web3Forms states that submissions may be retained for a maximum of three years from submission unless a shorter plan period applies or they are deleted earlier. Its copy does not automatically disappear when our own 12-month enquiry period ends. Contact us about deletion of a form submission; requests are assessed and passed to the provider where appropriate.
Core professional work records	Normally six years after the relevant piece of work is completed. This covers the necessary working papers, final outputs, instructions, queries, approvals and submission evidence. We retain information needed for continuing work, or a longer applicable legal period, for as long as that need lasts.
Engagement terms and standing authorities	For as long as they remain operative, and normally six years after they cease to apply or the relevant engagement ends, to evidence the scope and authority for our work.
AML customer due diligence and related records	Normally five years after the business relationship ends, or after completion of an occasional transaction where applicable. Personal information obtained under the Money Laundering Regulations is then deleted unless a permitted exception applies, such as another enactment, court proceedings, reasonable grounds for anticipated legal proceedings, or separate valid consent. Our ordinary six-year file rule does not override this requirement.
Client-controlled payroll or other processor records	In accordance with the client's lawful documented instructions and applicable agreement, including return or deletion when the service ends, unless law requires retention. Any records we must retain for our own distinct controller purpose are limited to that purpose.
Complaints and rights-request records	Only the material needed to demonstrate handling, findings and remedial action, normally six years after closure where necessary to meet accountability or claims needs. Unnecessary duplicates and sensitive supporting material are removed sooner.
Security, authentication and technical logs	Only as long as reasonably needed to run the service, investigate incidents, prevent abuse and evidence relevant access or approval events. Evidence needed for an actual incident or client file is separated from routine logs and retained under the relevant category.
Marketing choices and objections	While the relevant consent or preference is being relied on. A minimal suppression record may be retained for as long as needed to ensure that an objection or withdrawal continues to be respected.
Analytics and cookie records	Cookie or local-storage lifetimes are explained in section 10. Identifiable analytics information is retained only while needed to compare relevant website usage, diagnose issues and measure changes; provider retention limits also apply. We do not keep identifiable visitor data merely to preserve historical statistics that can be anonymised.

A legal or regulatory requirement, ongoing enquiry, dispute or reasonably anticipated claim can justify a different period. We record the reason, scope and review point rather than placing an indefinite hold on everything. Separate statutory identity-verification records, where such a service is lawfully undertaken, follow the retention requirement for that service.

Deletion from active systems and expiry from backups may occur at different times. Data awaiting backup expiry is not restored for ordinary use; where restoration is necessary, applicable deletion restrictions must be reapplied. We do not promise instantaneous erasure from every supplier system.

10. Website cookies, analytics and your choices

Essential storage and technical processing support website delivery, security, login sessions and remembering your privacy choices. Refusing optional analytics does not prevent an enquiry or access to the client service. Disabling essential storage in your browser can affect functions such as login.

For optional public website analytics, our chosen basis is your consent. Google Analytics 4 helps us understand visits, pages, referrals, devices and interactions. Microsoft Clarity helps us understand clicks, scrolling, page movement and session behaviour. These tools use identifiers and can process personal information even where reports do not show your name.

You can choose Accept analytics or Reject analytics. No choice means optional analytics remain off. You can change or withdraw your choice at any time using the Cookie choices controls in the website privacy notice. Withdrawal stops future consent-based tracking; it does not make earlier lawful processing unlawful. You can also delete existing cookies and site data using your browser settings.

Storage or service	Purpose and duration
Privacy choice stored on your device	Records whether you accepted or rejected optional analytics. The website uses local storage, which remains until it is changed, cleared by you or removed by the site; it is not a consent to unrelated processing.
Google Analytics cookies	Cookies such as _ga and the related property cookie distinguish visits and maintain session information. Google's standard _ga lifetime is up to two years; the browser and configured settings may shorten this. A new visit can refresh a persistent cookie.
Microsoft Clarity cookies	Cookies such as _clck and _clsk associate a browser and page views with usage analysis. Microsoft may also use its own identifiers under its published privacy terms. Lifetimes depend on the cookie, configuration and browser; you can inspect or remove them in your browser's site-data controls.
Portal login and security storage	Maintains authenticated access and protects the session. It lasts for the session or configured authentication period. Signing out and session expiry remove access, but retained security or signing evidence has a separate purpose under section 9.

Google and Microsoft may process information outside the UK; section 7 applies. Their own privacy and cookie information provides further detail: policies.google.com/privacy and privacy.microsoft.com. Public website analytics are not a reason to collect the contents of client accounting records, tax returns, passwords or identity documents.

A link to another website or platform takes you to a service with its own privacy arrangements. Contact us if a privacy control does not work or you need help making a choice.

11. Marketing, messages and recordings

We use your contact details to reply to enquiries and send necessary service messages. These are different from optional promotional communications. An enquiry or a privacy-notice acknowledgement is not automatic permission for unrelated marketing.

For electronic marketing to individuals, sole traders and other recipients protected by the relevant rules, we obtain consent unless a specific lawful exception applies. Where marketing to a corporate contact is permitted without consent, we rely on a proportionate legitimate interest and provide an opt-out. You can unsubscribe or contact us at any time; we will stop direct marketing when you object.

If you contact us through a messaging or social platform, the platform also processes information under its own arrangements. Avoid sending confidential records through public posts or comments. If a call or meeting is to be recorded or transcribed, we will tell you beforehand about the purpose, lawful basis, access and retention and obtain consent where required. This notice is not blanket permission to record you.

12. Confidentiality and security

We are responsible for applying proportionate technical and organisational safeguards to the information we hold. Access must be limited to people and service providers who need it for an authorised purpose, and the protections must reflect the sensitivity of the records. We use the portal and agreed document-sharing routes for the relevant workflows rather than treating the public enquiry form as a document vault.

No internet service can guarantee that an incident will never occur. We assess suspected losses or unauthorised access, take appropriate action and notify the ICO and affected people where the law requires. Please tell us promptly if you receive information in error, suspect unauthorised access or believe your contact details or portal account have been compromised.

Keep your login details private, use the security options available to you and verify unexpected requests for documents or payment details through a known contact route. Our responsibility for protecting information is not transferred to you by this advice.

13. Your information rights

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

- Explain how your information is used and provide access to it, including a copy of personal information you are entitled to receive.
- Correct inaccurate information and complete information that is incomplete.
- Erase information when there is no continuing lawful reason to retain it, or restrict particular uses while an issue is considered.
- Provide portable information where the right applies to automated processing based on consent or a contract with you.
- Respect an objection to legitimate-interest processing or direct marketing, or withdraw consent to a use based on consent.

- Provide the safeguards and human review required if a decision involving automated processing affects you.

Contact James Bodycombe by email, telephone or post. You do not have to use the portal or a particular form. We may need proportionate information to verify identity or clarify what is requested. Requests are normally free; a fee or refusal is used only where the law permits, with an explanation.

We respond without undue delay and normally within one calendar month, subject to any lawful adjustment or pause to the response period. Where the law permits an extension for complexity or the number of requests, we explain the reason within the initial period; the extension may be up to two further months.

Rights are not absolute. For example, a legal retention duty, another person's rights, legal privilege or a relevant statutory restriction can limit what may be deleted or disclosed. We explain a limitation where permitted. Outstanding fees do not by themselves remove your data protection rights.

14. Privacy complaints

Please contact James Bodycombe using the details at the start of this notice if you are concerned about how we have handled personal information. You can complain verbally or in writing; you do not need to make a subject access request first.

We acknowledge a data protection complaint within 30 days, start appropriate enquiries without undue delay from receipt, keep you informed as appropriate and explain the outcome and any corrective action. That acknowledgement period is not an extension of the separate time limit for responding to an information-rights request.

You can complain to the Information Commissioner's Office (ICO), the UK data protection regulator, at ico.org.uk/make-a-complaint/. You do not have to agree with our outcome, and this notice does not prevent you from contacting the ICO. A complaint about professional service may also fall under our separate client-care complaints procedure.

15. Keeping this notice current

We review this notice when our services, systems, providers, purposes or legal requirements change, and at least annually. Where a material change affects how your information is used, we provide appropriate updated information before the new use starts.

The website and client portal provide access to the current notice. We retain the version supplied with an engagement or other relevant collection point so that the information you were given can be identified. Updating this notice does not retrospectively create consent or alter a signed engagement.

Questions, requests or objections: James Bodycombe | jbodycombe@parkwoodlouvigny.co.uk | 07466 921648. Postal correspondence: Hectors House, Pankhurst Close, Exmouth, Devon EX8 2RN.