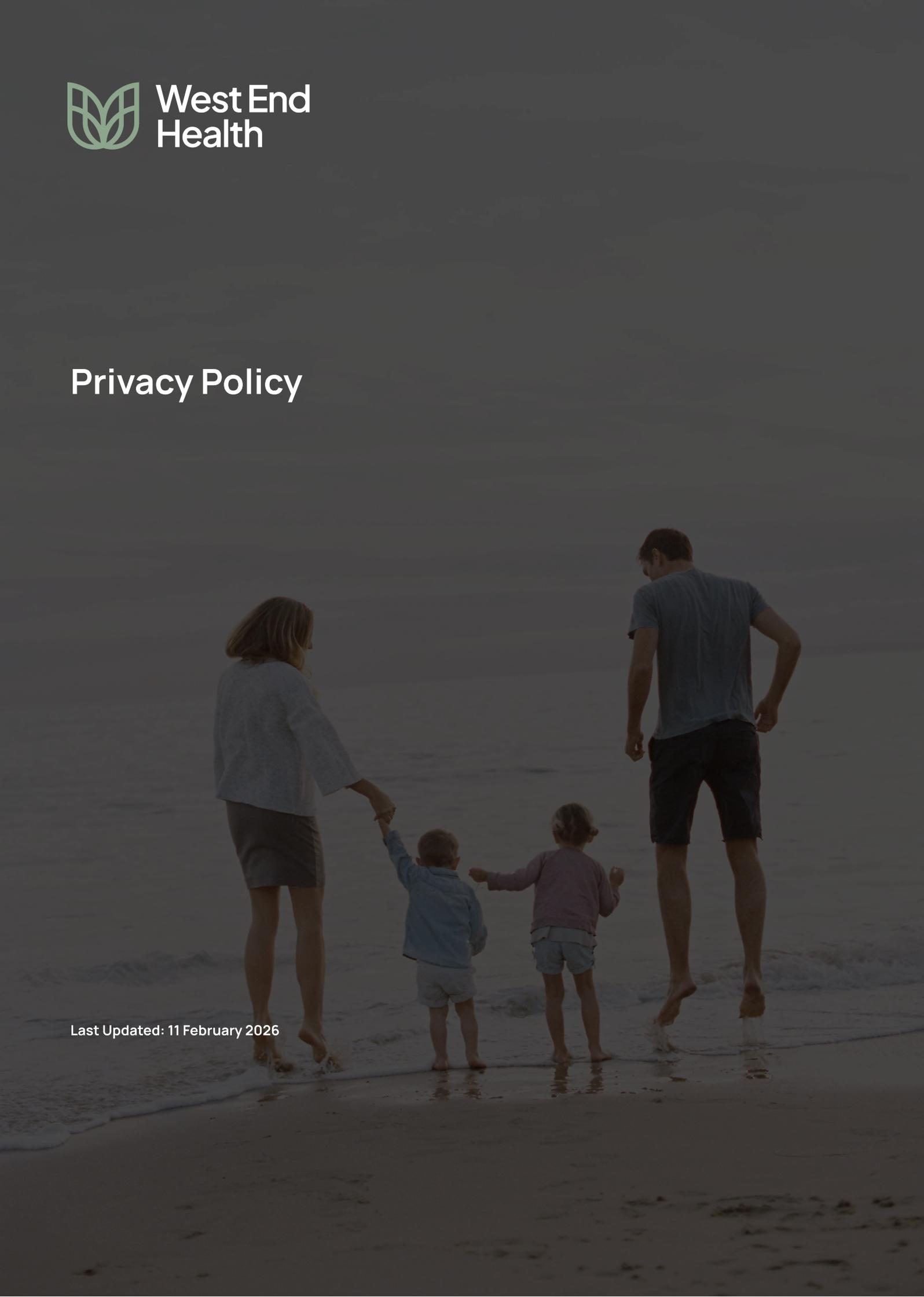


# Privacy Policy

Last Updated: 11 February 2026

A photograph of a family of four walking away from the camera on a beach at sunset. The mother is on the left, holding the hand of a young child. The father is on the right, also holding the hand of a young child. The children are in the middle, holding hands with each other. The scene is dimly lit, with the sun low on the horizon, creating a soft, golden glow over the water and sand.

This privacy notice explains how West End Health Limited (“we”, “us”, “our”) collects, uses, stores, and shares personal information, including health information, when you use our services or interact with us.

We are committed to protecting your privacy and handling your information safely and lawfully.

## Who we are

West End Health Limited is a private general practice providing primary medical services in Wales.

For data protection purposes, we are the Data Controller for the personal information we hold about you.

**Registered address:** 104 Conway Road, Colwyn Bay, Conwy LL29 7LL

**Telephone:** 01492 463453

**Email:** hello@westend.health

**Website:** <https://www.westend.health>

**Data Protection Lead:** Aaron Ferguson

**ICO registration number:** ZC010855

**HIW registration number:** HIW01086

## What information we collect

We may collect and process the following types of information:

### A. Identity and contact details

- Name, title, date of birth, gender.
- Home address, email address, telephone number.
- Next of kin / emergency contact details.
- NHS number (if you provide it).

### B. Health and care information (special category data)

This may include:

- Symptoms, medical history, diagnoses, examination findings.
- Prescriptions and medications.

- Allergies, vaccinations, test results, imaging, referrals, clinic letters.
- Lifestyle information relevant to clinical care.
- Notes from consultations and care plans.

## C. Appointment, communication, and service information

- Appointment dates/times and attendance.
- Messages you send us (email, web forms, portal messages).
- Call logs and call recordings.

## D. Billing and payment information

- Invoices, payment status, and transaction references. (We do **not** typically store full card details; payments are handled by payment providers.)

## E. Insurance / corporate membership information

- \* Insurer or membership provider details, authorisation codes, policy numbers.
- \* Employer details (where you receive services via a corporate arrangement).

## F. Website and device information

- IP address, device/browser details, pages visited, cookies.

## G. CCTV

- Video footage of visitors to our premises.

## How we collect your information

We collect information:

- **Directly from you** (forms, consultations, phone/email, online booking/portal)
- **From people/organisations involved in your care**, with your permission or where lawful (e.g., your NHS GP, other clinicians, pharmacies, labs, hospitals)
- **From insurers or corporate sponsors** (where they arrange/authorise payment for your care)

- **From public authorities** where required (e.g., safeguarding, legal obligations)

## How we use your information

We use your information to:

### Provide healthcare services

- Assess symptoms and medical history.
- Diagnose, treat, prescribe, and provide clinical advice.
- Arrange tests, interpret results, and make referrals.
- Coordinate care with other providers (with your agreement or where lawful/necessary).

### Manage appointments and communications

- Book and manage appointments.
- Send confirmations, reminders, and service messages (SMS/email/phone).

### Billing and administration

- Take payment, issue invoices/receipts.
- Process insurer/corporate authorisations where relevant.

### Quality, safety, and improvement

- Clinical audit, significant event review, complaints handling.
- Service planning and improving patient experience.

### Legal, regulatory, and professional obligations

- Meet record-keeping, tax/accounting, and regulatory requirements
- Respond to lawful requests from regulators or authorities.

### Protect our services and patients

- Information security, fraud prevention, safeguarding.

- Managing incidents and maintaining safe premises.

## Marketing

- Send service updates or newsletters only where you have opted in or where lawful to do so, and you can opt out at any time.

## Our lawful bases for processing

Data protection law requires us to have a lawful basis to process personal data. The lawful bases we rely on depend on what we are doing.

### Personal data (UK GDPR Article 6)

We typically rely on one or more of:

- **Contract:** providing private medical services you request, and associated administration.
- **Legal obligation:** compliance with legal/regulatory duties.
- **Legitimate interests:** running a safe, efficient medical service (balanced against your rights).
- **Consent:** where required (e.g., some marketing, optional services, certain disclosures).

### Health data (special category data – UK GDPR Article 9)

Health information is “special category data”. We process it primarily because it is necessary for:

- **\*Medical diagnosis and the provision of health care or treatment**, or the management of health care services, by/under the responsibility of a health professional.

We may also use other conditions in limited situations (e.g., emergencies or where you give explicit consent for a specific use).

## Sharing your information

We keep your information confidential. We share it only when necessary and lawful. We may share information with:

## A. Healthcare providers involved in your care

- Specialists, clinicians, hospitals, labs, imaging providers.
- Pharmacies and prescription services.

Where appropriate, we may (with your agreement) share relevant information with your **\*\*NHS GP\*\*** to support continuity of care.

## B. Service providers (data processors)

We may use vetted third parties to support our operations, such as:

- Clinical record systems / practice management systems.
- Patient portals and video consultation platforms.
- Laboratory and diagnostic providers.
- IT support, secure email/SMS providers.
- Payment processors, accountants, professional advisers.

These providers may only process your data on our instructions and must keep it secure.

## C. Insurers / corporate payers (where applicable)

We may share relevant administrative and (where necessary) clinical information to:

- Obtain authorisation, confirm eligibility, or process claims/payment.

We will share the minimum necessary.

## D. Regulators and authorities

We may share information when required or permitted by law, for example with:

- Healthcare regulators/inspectors (e.g., Healthcare Inspectorate Wales, where applicable).
- Courts, tribunals, law enforcement (when legally valid and necessary).
- Safeguarding authorities (if we believe someone is at risk of harm).

## If you withhold information

If you ask us not to share certain information or not to record certain information, we will consider your request. However, this may limit the care we can safely provide.

## International transfers

We aim to keep your information stored and accessed within the UK.

If any of our service providers transfer personal data outside the UK, we ensure appropriate safeguards are used (for example, adequacy regulations or contractual protections) to protect your information.

## How we keep your information secure

We use appropriate organisational and technical security measures, such as:

- Access controls and role-based permissions.
- Secure clinical systems and reputable service providers.
- Encryption where appropriate.
- Staff confidentiality obligations and training.
- Policies for secure handling, storage, and disposal of information.

No system is 100% secure, but we work to prevent unauthorised access, loss, misuse, or disclosure.

## How long we keep your information (retention)

We keep personal information only for as long as necessary for the purposes described above, including legal, clinical, and professional requirements.

- **Medical records:** We retain medical records in line with recognised health records retention guidance for GP-type records and medico-legal needs. In general, GP records are retained **\*\*for the lifetime of the patient and for a period after death\*\***, and electronic records may need to be retained for extended periods. Retention can be longer where required (e.g., investigations, complaints, litigation, or public inquiries).

- **Administrative and financial records:** We retain these for as long as needed for accounting, tax, and legal purposes.
- **CCTV (if used):** Typically retained for up to 90 days unless required for an incident investigation.

If you want more detail, contact us and we can provide our retention schedule.

## Your rights

You have rights under UK data protection law. These include:

- **Right to be informed** (this notice)
- **Right of access** to your personal data (often called a “Subject Access Request”)
- **Right to rectification** of inaccurate personal data
- **Right to erasure** (in some cases)
- **Right to restrict processing** (in some cases)
- **Right to data portability** (in some cases)
- **Right to object** (in some cases, especially for direct marketing)
- **Right to withdraw consent** (where we rely on consent)

**Important note for medical records:** Your rights are not absolute. For example, we may need to keep accurate clinical records for legal, clinical, and professional reasons even if you request deletion.

## How to make a request

Please contact our Data Protection Lead using the details in section 1. We may need to verify your identity before responding.

## Complaints

We encourage you to contact us first so we can try to resolve concerns quickly.

If you are unhappy with how we handle your information, you also have the right to complain to the UK regulator:

### Information Commissioner’s Office (ICO)

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

Telephone: 0303 123 1113

## Cookies and our website

If you use our website, we may use cookies and similar technologies for:

- Essential site functionality.
- Analytics (to understand how the site is used).
- Optional features (where enabled).

For details, see our [Website Privacy Policy](#).

## Emails, texts, and call recording

### Appointment reminders and service messages

We may contact you by SMS, email, or phone for appointment reminders and service-related communications.

### Clinical communications

If we communicate by email, please be aware that email is not always fully secure. We will use secure methods where appropriate (e.g., portals or encrypted services).

### Call recording

We record all telephone calls for training, monitoring and our mutual protection.

## CCTV

Where CCTV is used at our premises:

- It is used for safety and security.
- Signage will be displayed.
- Footage is accessed only by authorised staff.
- Footage is retained for up to 90 days unless needed for an incident.
- CCTV is not used in clinical or private areas.

## Children and young people

We provide services to children and young people in line with legal and professional standards. Where appropriate, we will involve parents/guardians, while also respecting confidentiality and the rights of competent young people.

## Changes to this notice

We may update this privacy notice from time to time. The latest version will be available on our website.