VISTA WELLBEING CIC

ALL TOGETHER, MORE SUPPORT

PUBLIC PRIVACY NOTICE & DATA PROTECTION POLICY

Website Publication Version | Compliant with UK GDPR, Data Protection Act 2018, PECR & Data (Use and Access) Act 2025

Document Field	Details
Data Controller	Vista Wellbeing CIC (ICO Registration: ZA324016)
Registered Address	116–118 Boutport Street, Green Lanes Shopping Centre, Barnstaple, EX31 1TD
Data Protection Lead	Anita Griggs, Data Protection Lead & Complaints Officer (info@vistawellbeing.org.uk)
Version & Effective Date	Version 1.2 (Public Website Edition) — Effective June 2026 (Reviewed Annually)

1. Who We Are & Our Service Boundaries

Vista Wellbeing CIC is a Community Interest Company limited by guarantee, governed by a Board of Directors. We are committed to protecting the privacy, dignity, and confidentiality of everyone who engages with our community programmes, referrals, and website.

Vista Wellbeing CIC delivers:

- Community-based physical activity and exercise support programmes
- Targeted falls prevention and postural stability programmes
- Health and wellbeing interventions

> **Clinical & Professional Boundaries Statement**
> Vista Wellbeing CIC is not a medical provider. We do not diagnose medical conditions, prescribe medication, provide medical treatment, or replace NHS clinical care. All exercise and wellbeing services are delivered safely within the competence of qualified instructors, with clear escalation pathways back to healthcare professionals where concerns arise.

2. Our Data Protection Principles

We process all personal information in strict accordance with the seven core principles of UK GDPR:

- **Lawfulness, Fairness & Transparency:** We only process personal data where a valid lawful basis exists and explain clearly how your data is used.
- **Purpose Limitation:** Information is collected for specified, explicit, and legitimate purposes and never used for unrelated commercial gain.

- **Data Minimisation:** We only collect information that is strictly necessary to deliver safe, effective services.
- **Accuracy:** We keep records accurate and up to date. Participants can view and update their own details at any time via their personal Membermojo membership dashboard.
- **Storage Limitation:** We retain personal data only for as long as necessary in line with our published retention schedule (Section 7).
- **Integrity & Confidentiality:** We protect personal and health data using strong technical, physical, and organisational security safeguards.
- **Accountability:** We maintain comprehensive governance records, staff training, and oversight to demonstrate legal compliance.

3. Privacy Notice: Information We Collect & How We Use It

This Privacy Notice applies to programme participants, prospective participants, referrers, volunteers, freelance instructors, website visitors, and anyone making an enquiry about our services.

3.1 Categories of Personal & Health Information We Process

- **Personal Data:** Full name, date of birth, postal address, email address, telephone number, emergency contact details, referral records, attendance logs, and communication history.
- **Health & Clinical-Type Data (Special Category Data):** Where necessary for safe exercise delivery, we process relevant medical conditions, mobility and functional ability, falls history and falls risk assessments, relevant medications, exercise contraindications, PAR-Q+ screening outcomes, blood pressure (where taken), and strength, balance, or wellbeing outcome measures.
- **Website & Technical Data:** IP address, browser type, device information, page usage statistics, and cookie preferences (see our Website Cookie Policy in Section 9).

3.2 How We Receive Information

We receive information directly from you (via registration forms, PAR-Q+ health screenings, intake consultations, our website, or your Membermojo account) as well as from authorised referral partners—including General Practitioners (GPs), Social Prescribing Link Workers, NHS community teams, Allied Health Professionals, Local Authority services, and voluntary sector partners.

3.3 Lawful Bases for Processing (UK GDPR Articles 6 & 9)

We never sell your personal data. Depending on the activity, we rely on the following lawful bases:

- **Consent — Article 6(1)(a):** Used for optional photography, video recordings, and optional marketing updates. You may withdraw consent at any time.
- **Contract — Article 6(1)(b):** Necessary to manage your bookings, deliver agreed sessions, and administer participation.
- **Legal Obligation — Article 6(1)(c):** Necessary to comply with statutory safeguarding duties, financial accounting laws, and regulatory obligations.
- **Legitimate Interests — Article 6(1)(f):** Necessary for safe service administration, pre-exercise risk screening, referral management, programme evaluation, and governance—always balanced against your individual rights and reasonable expectations.
- **Special Category Health Data — Article 9 UK GDPR:** Because health data is Special Category Data, we also satisfy a separate Article 9 condition—primarily Article 9(2)(h) (Provision of health or social care or management of health/social care systems), alongside Article 9(2)(a) (Explicit Consent where required), Article 9(2)(g) (Substantial Public Interest for safeguarding), and Article 9(2)(c) (Vital Interests in a medical emergency).

3.4 Who We Share Information With

We treat your records as strictly confidential and only share relevant information where lawful and proportionate with:

- NHS referrers (such as GPs, Social Prescribers, and NHS community health teams) to coordinate your care pathway or escalate new clinical symptoms
- Emergency services (999) in the event of a medical emergency during a session to protect your vital interests
- Statutory safeguarding teams where required to protect an adult or child at risk
- Local authority or NHS commissioners and grant funders (using anonymised statistical reports unless identifiable reporting is contractually required and notified to you)
- Approved data processors operating under UK GDPR Article 28 contracts (such as Membermojo for secure membership records and CookieYes for website cookie consent)

4. Health Screening, Referrals & Safe Participation

Before joining any Vista Wellbeing CIC activity programme, participants complete a PAR-Q+ health screening and functional/falls risk consultation with a qualified instructor. Your records are stored securely in Membermojo (membermojo.co.uk), where you can log in at any time to view or update your health and medication details.

If you experience new symptoms (such as chest pain, unexplained breathlessness, or dizziness), if your health risks increase, or if additional medical advice is needed, we may pause your participation and refer you back to your GP, Social Prescriber, NHS team, or Emergency Services using secure encrypted transfer methods.

5. Your Individual Rights & Subject Access Requests (2026 Rules)

Under UK data protection law (including the UK GDPR and the Data (Use and Access) Act 2025), you have the right to:

- **Right to Be Informed:** Understand clearly how we collect and use your personal information.
- **Right of Access (DSAR):** Request a copy of the personal data we hold about you (or view your membership record directly in Membermojo).
- **Right to Rectification:** Ask us to correct inaccurate or incomplete information.
- **Right to Erasure:** Request deletion of your personal data where there is no overriding legal, safety, or insurance requirement to retain it.
- **Right to Restrict Processing:** Ask us to limit how we use your data in certain circumstances.
- **Right to Object:** Object to processing based on legitimate interests (Article 21) or direct marketing.
- **Right to Data Portability:** Receive certain personal data in a structured, commonly used electronic format.
- **Automated Decision-Making:** Vista Wellbeing CIC does not currently use automated decision-making or AI risk-scoring tools. Should we consider introducing any digital risk-scoring tools in future, we will conduct a Data Protection Impact Assessment (DPIA) and inform participants beforehand.

How to Make a Data Request

- **Submitting a Request:** You can make a request by email (info@vistawellbeing.org.uk), by post (116–118 Boutport Street, Barnstaple, EX31 1TD), or verbally. No specific form is required, though an optional DSAR Form is available on our website and on request.
- **Identity Verification:** We may ask to verify your identity (e.g. driving licence, passport, or utility bill). Identification documents are destroyed immediately once verified and are never retained on file.
- **Timeframes & 2026 Rules:** We normally respond within one calendar month. Under the Data (Use and Access) Act 2025, if a request is unclear or overly broad, we may ask you to clarify what information you need, pausing the one-month clock until clarification is received. We conduct reasonable and proportionate searches across our active systems and redact third-party personal data where required.

6. How We Keep Your Information Secure

We protect personal and health data using appropriate technical, physical, and organisational safeguards, including:

- Strong password protection, Multi-Factor Authentication (MFA), and strict role-based, need-to-know access controls

- Encrypted cloud storage on UK/EEA-compliant platforms (Membermojo, Microsoft OneDrive/SharePoint, and Google Drive)
- Secure encrypted transfer (such as NHSmail or password-protected files) when sharing clinical or discharge updates with NHS referrers
- Locked physical filing cabinets at our Barnstaple office for any temporary paper forms, followed by cross-cut shredding or confidential waste disposal
- Live website firewall and malware monitoring (MalCare)
- Mandatory confidentiality agreements and annual data protection training for all Directors, instructors, staff, and volunteers
- Strict incident response procedures, including reporting high-risk data breaches to the Information Commissioner's Office (ICO) within 72 hours and notifying affected individuals where required

7. How Long We Keep Your Information (Retention Schedule)

We retain personal data only for as long as necessary to deliver services safely, meet insurance and legal requirements, and satisfy regulatory standards. Once retention periods expire, records are permanently deleted or securely shredded.

Record Type	Standard Retention Period	Disposal Method
Participant registration, health / PAR-Q+, falls risk, referral & outcome records	7 years after last contact	Secure deletion / cross-cut shredding
Outcome measures (fully anonymised)	May be retained longer for service evaluation	Not applicable (non-identifiable)
Consent forms & electronic consent records	7 to 8 years after last engagement	Secure deletion / cross-cut shredding
Website enquiries	6 months	Secure deletion
Safeguarding records	Until child reaches 25th birthday (or 7+ years for adult safeguarding)	Secure deletion / cross-cut shredding
Incident / accident reports & insurance records	6 years (40 years for Employer Liability insurance)	Secure deletion / cross-cut shredding
Data protection complaints & data breach records	6 years after closure	Secure deletion / cross-cut shredding
Data Subject Access Request (DSAR) records	2 years after completion	Secure deletion / cross-cut shredding
Volunteer & freelance instructor records	6 years after involvement / contract ends	Secure deletion / cross-cut shredding
Financial records	6 years plus current financial year	Secure deletion / cross-cut shredding

8. Direct Marketing, Photography & Media Preferences

- **Electronic Direct Marketing (PECR):** Essential operational messages about your booked classes (such as venue changes, cancellations, or annual PAR-Q+ health review reminders) are sent as service communications. Promotional newsletters or event invitations are only sent where you have actively opted in (or under strict PECR service soft opt-in rules with an immediate opt-out). Every marketing email includes an easy unsubscribe link, and opt-outs are honoured immediately.
- **Photography & Media Consent:** Photography and video consent is entirely optional and separate from programme participation. You can choose separately whether to allow internal session photos, session videos, or

public website/social media use, ask to step out or be blurred out at any session, and change your preferences at any time via Membermojo or your instructor.

9. Website Cookie Policy

Cookies are small text files placed on your device when you visit our website (www.vistawellbeing.org.uk). We manage cookie preferences transparently using our CookieYes consent banner in accordance with PECR and the Data (Use and Access) Act 2025:

Cookie / Provider	Category	Purpose	Duration
cookieyes-consent (CookieYes)	Strictly Necessary (Always Active)	Remembers your cookie banner choices so you are not asked on every page.	1 year
mc_session / Security (MalCare)	Strictly Necessary (Always Active)	Protects our website from malicious traffic, bots, and cyber attacks.	Session / 24 hours
_ga / _ga_* (Google Analytics, if active)	Analytics (Opt-In Only)	Collects anonymous statistical data on page visits and navigation only if you click 'Accept'.	Up to 12 months
Third-Party Embeds (e.g. YouTube / Maps)	Marketing / Third-Party (Opt-In Only)	Blocked by default until you give explicit opt-in consent via our cookie banner.	Varies by provider

You can change or withdraw your cookie preferences at any time by clicking the 'Cookie Settings' link at the bottom of any webpage, or by adjusting your web browser settings.

10. How to Contact Us or Make a Data Protection Complaint

If you have any questions about this Privacy Notice, wish to exercise your individual rights, or want to raise a data protection complaint, please contact our Data Protection Lead:

Contact Route	Details
Data Protection Lead & Complaints Officer	Anita Griggs, Vista Wellbeing CIC
Email (Electronic Complaints & Requests)	info@vistawellbeing.org.uk
Postal Address	Vista Wellbeing CIC, 116–118 Boutport Street, Green Lanes Shopping Centre, Barnstaple, EX31 1TD
Our Complaints Service Standards	Under the Data (Use and Access) Act 2025, you may submit complaints electronically, in writing, or verbally (an optional Complaint Form is available on our website). We acknowledge all complaints within 5 working days and provide a full response within 1 calendar month. Unresolved concerns may be escalated internally to Sue Ward (Governance & Safeguarding Lead) and the Board of Directors.

Your Unconditional Right to Complain to the ICO

You have the right to lodge a complaint directly with the UK's independent data protection regulator, the Information Commissioner's Office (ICO), at any time without first using our internal complaints process:

Website: www.ico.org.uk | Telephone: 0303 123 1113 | Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF