

**Unity of Migrant Workers (UMW)
Data Protection Policy**

Version: 1.0

Approved by Board on 01/2/2025

Next review date: 01/01/2026



1. Introduction

Unity of Migrant Workers (“UMW”, “we”, “us”) is committed to protecting the personal data of everyone we work with, including our members, service users, volunteers, staff, trustees, partners and supporters.

This policy explains how we collect, use, store and share personal data in line with:

- The UK General Data Protection Regulation (“UK GDPR”); and
- The Data Protection Act 2018.

We aim to be:

- Lawful, fair and transparent in the way we process data
- Accountable for our decisions and practices
- Respectful of people’s rights and expectations.

This policy applies to all trustees, staff, volunteers, sessional workers and anyone else processing personal data on behalf of UMW.

2. Who we are

Organisation name: Unity of Migrant Workers

Legal status: Registered charity in England and Wales

Charity number: 1213132

Registered address: 53 Stoke Newington High Street, London, N16 8EL

Website: <https://umwb.org.uk>

Contact email for data protection: info@igeb.org.uk

UMW is the “data controller” for the personal data it processes. This means we decide how and why personal data is used.

3. What personal data we collect

We only collect data that we need to run our services, manage our organisation and meet our legal obligations. This may include:

3.1 Service users, participants and members

- Name and contact details (address, phone number, email)
- Date of birth, gender and preferred language
- Immigration status and nationality (where relevant and provided)
- Information about family, caring responsibilities or household
- Attendance at activities, courses, events and appointments
- Support needs and notes about the help we have provided
- Feedback, complaints and compliments.

3.2 Staff, volunteers and trustees

- Name, contact details and emergency contacts
- Application forms, CVs and references
- Right to work information and identity documents
- Criminal records checks (DBS) where required
- Bank details for payroll or reimbursement
- Records of training, supervision, performance and safeguarding.

3.3 Donors, supporters and partners

- Name and contact details
- Donation history and Gift Aid information (if applicable)
- Records of communications, meetings and partnership work.

3.4 Special category data

We may collect special category data where necessary and lawful, for example:

- Health information (e.g. access needs, disabilities, mental health)
- Racial or ethnic origin
- Political opinions or trade union membership (in very limited cases where relevant)
- Religious or philosophical beliefs.

We collect and use special category data only where:

- We have the person's explicit consent; or
- It is necessary for substantial public interest (for example safeguarding, promoting equality, or providing targeted support to migrants and minoritised communities), and we have appropriate safeguards in place.

4. How we collect data

We collect personal data in several ways, including:

- Directly from individuals (for example registration forms, feedback forms, email, phone, website contact forms, social media)
 - Via referrals from trusted partners or agencies (with appropriate consent where needed)
 - From publicly available sources (for example Companies House, Charity Commission) for due diligence and governance purposes.
-

5. Our lawful bases for processing

We process personal data under the following lawful bases in Article 6 UK GDPR:

- **Consent** – where individuals have clearly agreed to us processing their data (for example email newsletters, photos for publicity).
- **Contract** – to fulfil an agreement with the person (for example employment, volunteer agreement, sessional work contracts).
- **Legal obligation** – to meet legal or regulatory requirements (for example safeguarding, HMRC/Gift Aid, employment law, health and safety).
- **Vital interests** – in rare situations to protect someone's life or serious welfare.
- **Public task / legitimate interests** – where processing is necessary to deliver our charitable purposes, manage our services, secure funding and evaluate impact, and where this is not overridden by the individual's rights.

For **special category data** we rely on:

- Explicit consent; and/or
 - Substantial public interest (for example safeguarding of children and adults at risk, equality of opportunity, support to disadvantaged or marginalised individuals) under the Data Protection Act 2018.
-

6. How we use personal data

We use personal data to:

- Provide and manage our services, projects and activities
- Assess eligibility and suitability for activities or support
- Monitor participation, outcomes and impact
- Manage safeguarding, welfare and risk
- Recruit, support and manage staff, volunteers and trustees
- Communicate with participants, partners, funders and supporters
- Manage our finances, fundraising and reporting obligations
- Meet our legal, regulatory and insurance requirements
- Develop and improve our programmes based on feedback and evaluation.

We will not use personal data for purposes that are incompatible with these aims, unless we are required to do so by law.

7. Data sharing

We only share personal data where it is necessary, lawful and proportionate. This may include sharing with:

- Funding bodies (for example anonymised or aggregated statistics; occasionally limited personal data if required by the funder agreement)
- Partner organisations we work with to deliver services (under appropriate agreements)
- External professional services (for example payroll provider, auditors, insurers, IT support), who act as “data processors” and are bound by contracts to protect personal data
- Safeguarding agencies (for example local authority, police, social services) where there are concerns about harm or risk
- HMRC and other regulatory bodies where required by law.

We do not sell personal data and we do not allow third parties to use it for their own marketing.

Where possible, we share data in an anonymised or pseudonymised form.

8. International transfers

Our core systems and data storage are based in the UK or EEA where possible. If we use services that may involve transfer of personal data outside the UK/EEA (for example certain cloud services), we will ensure that appropriate safeguards are in place, such as:

- Adequacy regulations; or
 - Standard Contractual Clauses; or
 - Other legally recognised safeguards.
-

9. Data retention

We keep personal data only for as long as necessary for the purposes for which it was collected, and in line with legal and funder requirements. As a general guide (subject to specific project or legal requirements):

- Service user records: normally up to 6 years after last contact
- Safeguarding records: at least 6 years after case closure, sometimes longer depending on guidance
- HR, staff and volunteer records: up to 6 years after employment/engagement ends (longer for pension or accident records)

- Financial records (including donations and Gift Aid): 6 years after the end of the relevant financial year.

At the end of the retention period, data will be securely destroyed or anonymised so it can no longer identify individuals.

10. Data security

We take appropriate technical and organisational measures to protect personal data, including:

- Limiting access to personal data on a “need to know” basis
- Using password-protected devices and accounts
- Keeping paper records in locked storage where practicable
- Training trustees, staff and volunteers on data protection and confidentiality
- Using secure methods for transferring data (for example encrypted email where appropriate)
- Having procedures in place to respond to data breaches or suspected breaches.

Everyone working with UMW has a duty to keep personal data safe and confidential.

11. CCTV and photography

If we use **CCTV** at our premises, we will:

- Display appropriate signage
- Use footage only for security, safety and safeguarding purposes
- Retain footage for a limited period unless required for investigation.

If we take **photos or videos** at events or activities:

- We will seek appropriate consent where individuals can be clearly identified
- We will explain how images will be used (for example website, social media, reports)
- People can withdraw their consent at any time, and we will stop using their image for new materials.

If we are not using CCTV at a particular site, we will make this clear in local signage or notices.

12. Individual rights

Individuals have the following rights under UK GDPR, subject to conditions:

- **Right to be informed** – to know how their data is used (for example this policy, privacy notices)
- **Right of access** – to request a copy of the personal data we hold about them
- **Right to rectification** – to ask us to correct inaccurate or incomplete data
- **Right to erasure** – to request deletion of their data in certain circumstances
- **Right to restrict processing** – to ask us to limit how their data is used
- **Right to data portability** – to receive data in a structured, commonly used format (where applicable)
- **Right to object** – to object to certain types of processing (for example direct marketing)
- **Rights in relation to automated decision-making and profiling** – UMW does not currently carry out automated decision-making.

Requests to exercise these rights should be made in writing (email or post) using the contact details in section 14. We will respond within one month where possible, and explain if we need more time or if any exemptions apply.

13. Data breaches

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If a breach is suspected:

- It must be reported immediately to the Data Protection Lead or Chair of Trustees.
 - We will investigate, take steps to contain and remedy the breach, and keep appropriate records.
 - Where legally required, we will notify the Information Commissioner's Office (ICO) within 72 hours and, where appropriate, inform affected individuals.
-

14. Contact and complaints

If you have any questions, concerns or requests about this policy or how we handle personal data, please contact:

Data Protection Lead

Unity of Migrant Workers
53 Stoke Newington High Street
London
N16 8EL

Email: info@igeb.org.uk

You also have the right to raise concerns with the **Information Commissioner's Office (ICO)** at any time:

Website: ico.org.uk
Phone: 0303 123 1113

15. Review

This policy will be reviewed at least once every two years, or sooner if there are significant changes in our activities, the law or regulatory guidance.