

GDPR and Data Protection Policy

UK GDPR · DATA PROTECTION ACT 2018

Policy Owner	Board of Trustees
Data Protection Lead	Julie Khan-Muhammad
Version	1.0
Effective Date	2026
Next Review Date	2027

Contents

1 Policy Statement	9 Data Retention and Disposal
2 Purpose	10 Data Security
3 Scope	11 Data Breaches
4 The UK GDPR Principles	12 Data Sharing and Third Parties
5 Lawful Basis for Processing	13 Responsibilities
6 Special Category Data	14 Related Legislation and Documents
7 Individual Rights	15 Feedback
8 Consent	16 Approval and Review Details

1 Policy Statement

Unique Minds (LAMEHLAK, Charity No. 1206326) is committed to protecting the privacy and personal data of all individuals it works with, including service users, carers, families, staff, volunteers, and partner organisations. The organisation recognises that the responsible and lawful handling of personal data is fundamental to the trust placed in it by the people it supports.

This policy applies to all staff, trustees, volunteers, contractors, and any individual processing personal data on behalf of Unique Minds. Non-compliance with this policy may result in disciplinary action and, in serious cases, referral to the Information Commissioner's Office (ICO).

We handle personal data with care, transparency, and respect for every individual.

2 Purpose

This policy sets out how Unique Minds collects, uses, stores, shares, and disposes of personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Given that Unique Minds works with people living with dementia and their carers – individuals who may be particularly vulnerable. The protection of personal data is not only a legal obligation but a fundamental aspect of delivering a safe and trustworthy service.

The policy also ensures that the organisation meets its obligations as a registered data controller with the Information Commissioner's Office (ICO).

3 Scope

This policy applies to all personal data processed by or on behalf of Unique Minds, including:

- ✓ Personal data relating to service users, carers, and family members
- ✓ Staff, volunteer, and trustee personal data
- ✓ Data collected through the website, referral forms, and CRM system
- ✓ Data shared with or received from partner organisations, statutory agencies, and funders
- ✓ Any data processed during outreach activities or home visits

4 The UK GDPR Principles

All personal data processed by Unique Minds must be handled in accordance with the six principles of the UK GDPR:

Principle	What this means for Unique Minds
Lawfulness, fairness and transparency	We will only collect and use data for legitimate purposes, and we will be open with individuals about how their data is used.
Purpose limitation	Data will only be collected for specified, explicit, and legitimate purposes and will not be used in ways incompatible with those purposes.
Data minimisation	We will only collect the data we genuinely need – no more than is necessary for the purpose.
Accuracy	We will keep personal data accurate and up to date, correcting or deleting inaccurate data promptly.
Storage limitation	Personal data will not be kept longer than is necessary. Retention periods are set out in our retention schedule.
Integrity and confidentiality	Data will be kept secure and protected against unauthorised access, loss, or destruction through appropriate technical and organisational measures.

5 Lawful Basis for Processing

Unique Minds must identify and document a lawful basis before processing any personal data. The lawful bases most commonly applicable to our work are:

- ✓ Consent, where an individual has given clear, informed, and freely given consent to their data being processed for a specific purpose
- ✓ Legitimate interests, where processing is necessary for the legitimate interests of the organisation, provided these are not overridden by the rights and freedoms of the individual
- ✓ Legal obligation, where processing is necessary to comply with a legal requirement, such as safeguarding duties
- ✓ Vital interests, where processing is necessary to protect someone's life, particularly relevant in safeguarding situations
- ✓ Public task, where applicable in connection with statutory or public functions

The lawful basis for each category of data processing will be documented in the organisation's data processing register.

6 Special Category Data

Unique Minds processes special category data as part of its core service delivery. Special category data includes information about health conditions, disabilities, and other sensitive personal characteristics.

Given that the primary service users are people living with dementia, health data is central to the Wayfinder service. This data will only be processed where:

- ✓ The individual has given explicit consent, or
- ✓ Processing is necessary for the provision of health or social care services, or
- ✓ Processing is necessary for reasons of substantial public interest under applicable law

All special category data must be treated with the highest level of care, stored securely, and only accessed by staff who require it for their role. Special category data must never be shared without explicit consent or a clear legal basis.

7 Individual Rights

Under the UK GDPR, individuals have the following rights in relation to their personal data. Unique Minds will ensure that these rights can be exercised effectively:

Right	Summary
Right to be informed	Individuals must be told how their data is used, at the point of collection (via a privacy notice).
Right of access	Individuals can request a copy of the data held about them (Subject Access Request). Unique Minds will respond within one month.
Right to rectification	Individuals can ask for inaccurate or incomplete data to be corrected.
Right to erasure	Individuals can request their data is deleted, subject to legal or safeguarding obligations.
Right to restrict processing	Individuals can ask Unique Minds to limit how their data is used in certain circumstances.
Right to data portability	Where applicable, individuals can request their data in a portable format.
Right to object	Individuals can object to processing based on legitimate interests or for direct marketing purposes.

8 Consent

Where consent is the lawful basis for processing, Unique Minds will ensure that consent is:

- ✓ Freely given, individuals must not be pressured or coerced into giving consent
- ✓ Specific, consent must relate to a clearly defined purpose
- ✓ Informed, individuals must be provided with clear information about how their data will be used before giving consent

- ✓ Unambiguous, consent must be a positive opt-in action, not assumed from inaction or pre-ticked boxes

Consent can be withdrawn at any time. Where consent is withdrawn, processing for that purpose must cease promptly. Records of consent must be maintained.

Special note for dementia service users / Where a service user has reduced mental capacity, the Mental Capacity Act 2005 principles will be applied. Staff must assess capacity on a decision-by-decision basis and, where appropriate, involve carers or legal representatives in line with best interests procedures.

9 Data Retention and Disposal

Personal data will not be kept for longer than is necessary for the purpose for which it was collected. Unique Minds will maintain a data retention schedule setting out retention periods for each category of data.

Indicative Retention Periods

Data Category	Indicative Retention Period
Service user case records	7 years after last contact, or until the individual's 25th birthday if they were a child at the time of access
Staff employment records	6 years after employment ends
Volunteer records	3 years after volunteer role ends
Financial and grant records	7 years
Accident and incident records	3 years minimum (RIDDOR reportable: 3 years from date of incident)
Safeguarding records	Retained in line with local authority guidance — do not delete without seeking advice
Marketing and communications consent	Until consent is withdrawn or 3 years of inactivity

When data is no longer required, it must be disposed of securely. Paper records must be shredded. Electronic records must be permanently deleted. Disposal must be documented.

10 Data Security

Unique Minds will implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or disclosure.

Technical Measures

- ✓ Password-protected devices and systems — all computers and devices must require a password or PIN to access
- ✓ Secure Wi-Fi — the centre's Wi-Fi must be password protected and a separate guest network used where appropriate
- ✓ Encrypted storage for sensitive data wherever practicable
- ✓ Regular software updates and security patches applied to all devices
- ✓ Anti-virus and firewall protection maintained on all devices
- ✓ CRM system with role-based access controls — staff will only have access to data relevant to their role

Organisational Measures

- ✓ Clear desk and clear screen policy, personal data must not be left visible or unattended
- ✓ Paper records stored in locked filing cabinets with restricted access
- ✓ Visitor access to the centre must be controlled and unauthorised individuals must not have access to areas where personal data is stored or processed
- ✓ Staff must not share passwords, login credentials, or access to systems
- ✓ Personal data must not be transmitted via unsecured email, encrypted email or secure file transfer must be used for sensitive data
- ✓ Mobile working, staff accessing data remotely or during outreach must ensure devices are kept secure and not used in public settings where screens could be observed

11 Data Breaches

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All staff and volunteers must report suspected data breaches immediately to the Data Protection Lead.

Response Procedure

- ✓ The breach must be contained as quickly as possible: for example, by revoking access or recovering lost documents
- ✓ The Data Protection Lead must assess the risk to individuals affected
- ✓ Where the breach is likely to result in a risk to the rights and freedoms of individuals, it must be reported to the ICO within 72 hours of becoming aware of it
- ✓ Where the breach is likely to result in a high risk to individuals, those individuals must also be notified without undue delay
- ✓ All breaches, whether reportable or not, must be documented in the breach register

ICO CONTACT

Information Commissioner's Office: 0303 123 1113 | www.ico.org.uk | Report a breach: ico.org.uk/report-a-breach

12 Data Sharing and Third Parties

Unique Minds may need to share personal data with third parties while delivering services. This includes referral agencies, statutory authorities, NHS partners, funders, and technology providers (including the CRM system supplier).

Data sharing will only take place where:

- ✓ There is a lawful basis for doing so
- ✓ It is necessary and proportionate to the purpose
- ✓ A data sharing agreement or data processing agreement is in place where required
- ✓ The recipient organisation handles the data securely and in compliance with UK GDPR

Where personal data is shared for safeguarding purposes, it may be shared without consent where there is a legal obligation or vital interest basis. This must be documented.

Unique Minds will not sell, rent, or otherwise trade personal data with any third party for commercial purposes.

13 Responsibilities

Board of Trustees

The Board has overall accountability for data protection compliance and must ensure this policy is implemented and reviewed effectively.

Data Protection Lead

The Data Protection Lead is responsible for overseeing compliance with this policy, responding to data subject requests, managing data breaches, liaising with the ICO, and ensuring staff receive appropriate training. The organisation must register with the ICO as a data controller.

Centre Director

The Centre Director is responsible for embedding data protection practices into day-to-day operations, ensuring staff and volunteers are trained, and that data is handled appropriately across all centre activities.

All Staff and Volunteers

All staff and volunteers must:

- ✓ Handle personal data only in accordance with this policy and their role
- ✓ Report any data breaches or suspected breaches immediately

- ✓ Complete data protection training at induction and as required
- ✓ Not share, misuse, or access personal data beyond what is required for their role

14 Privacy Notice — Staff and Volunteer Data

Unique Minds collects and processes personal data relating to staff and volunteers in order to manage employment and volunteering relationships effectively. The following table sets out what data is collected, why, and how it is used.

What information is collected?	Name, contact details, emergency contact information, date of birth, bank details and National Insurance number, application forms, references, DBS check results, training records
Who collects it?	The Centre Director or designated HR lead on behalf of Unique Minds
How is it collected?	Application forms, contracts, paper and electronic records
Why is it collected?	To manage the employment or volunteering relationship, process payments, meet legal obligations including safeguarding, and ensure staff safety at work
How will it be used?	To process payroll, manage HR matters, maintain training records, and for emergency contact purposes
Who will it be shared with?	Payroll/finance providers for salary processing; statutory authorities where required by law (e.g. DBS, HMRC); senior management in cases of emergency
International transfers?	No personal data will be transferred outside the UK
Retention period	6 years after employment ends (see data retention schedule)
Data Controller contact	Centre Director, Unique Minds, 100–102 High Street, Stourbridge, DY8 1EQ

15 Consequences of Failing to Comply

Unique Minds takes compliance with data protection law very seriously. Failure to comply with this policy or UK GDPR may result in significant harm to individuals, damage to the organisation's reputation, and regulatory action by the Information Commissioner's Office.

Any member of staff or volunteer who knowingly or recklessly breaches this policy may face disciplinary action in accordance with the organisation's disciplinary procedures. Serious breaches may result in dismissal. In some circumstances, individual breaches of data protection law may also constitute a criminal offence.

If you have any questions about this policy or are unsure how it applies to your role, contact the Data Protection Lead before taking any action.

16 Related Legislation and Documents

This policy is underpinned by:

- ✓ UK General Data Protection Regulation (UK GDPR)
- ✓ Data Protection Act 2018
- ✓ Human Rights Act 1998
- ✓ Mental Capacity Act 2005
- ✓ Care Act 2014
- ✓ Freedom of Information Act 2000 (where applicable to public interest activities)

This policy should be read alongside:

- ✓ Safeguarding Adults Policy
- ✓ Safeguarding Children Policy
- ✓ Health & Safety Policy
- ✓ Confidentiality and Information Sharing Policy
- ✓ Complaints and Feedback Policy

17 Feedback

Feedback on this policy is welcomed from staff, volunteers, service users, carers, and partner organisations. Feedback can be provided through supervision, team meetings, or directly to the Data Protection Lead and will be used to inform future reviews and improvements.

18 Approval and Review Details

This policy will be formally reviewed annually, or sooner if there are changes to legislation, ICO guidance, or organisational practice.

Policy Name	GDPR and Data Protection Policy
Organisation	Unique Minds
Policy Owner	Board of Trustees
Data Protection Lead	Julie Khan Muhammad
ICO Registration Number	
Approved By	Board of Trustees
Date Approved	
Review Frequency	Annually or as required
Next Review Date	10.06.2027
Version Number	1.0
Last Updated	10.06.2026