DMNW Policy Cover Sheet

Policy Name GDPR Policy

Target Audience: *(Please tick as appropriate)*

x	Staff
x	Trustees
x	Volunteers

Date Authorised:	**October 2025**
Authorised By:	**DMNW Board**
Review Date:	**2030**
Changes Made by CEOs due to legislation/ operational requirements:[1]	
Key legislations and guidance used to inform policy / strategy:	
This policy has been updated in line with the new Data Use and Access Act requirements 2025. Data (Use and Access) Act 2025: data protection and privacy changes - GOV.UK	

[1] As agreed by DMNW Board 6th March 2024

Table of Contents

Policy Statement

Diversity Matters North West (DMNW) is committed to protecting personal data and ensuring it is handled lawfully, fairly, and securely. This policy outlines how DMNW collects, uses, stores, and shares personal data in line with UK GDPR, the Data Protection Act 2018, and the Data Use and Access Act 2025.

Scope

DMNW will remain the data controller for the information it collects and holds. DMNW, its board members, staff and volunteers will be personally responsible for processing and using personal information in accordance with the current legislation. All board members, staff and volunteers working with DMNW who have access to personal information, will be expected to read and comply with this policy. Non-compliance with this policy could result in disciplinary action, loss of job (or volunteering placement), personal fines and potentially imprisonment.

Definitions

Data Controller – The person who (either alone or with others) decides what personal information Diversity Matters North West will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Use and Access Act 2025- is a UK law that introduces updates to existing data protection legislation, including the UK GDPR and the Data Protection Act 2018. It does not replace these laws but modifies and supplements them to make data use more efficient, transparent, and secure.

***Data Protection Impact Assessments (DPIA*)** - is a process to help you identify and minimise the data protection risks of a project.

Data Protection Lead – The person(s) responsible for ensuring that DMNW follows its data protection policy and complies with legislation.

Individual/Service User – The person whose personal information is being held or processed by DMNW for example: a client, an employee, or member.

Information Commissioner (ICO)– The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g., name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, including service users, individual volunteers or employees

Sensitive Data – refers to data about race, ethnic origin, political opinion, religion, trade union membership genetic data, biometrics, health data, sex life or sexual orientation.

Policy Content

GDPR Key Principles

The Data Protection Legislation sets out seven key principles (Article 5(1)) which are summarised as follows:

Lawfulness – This means making sure there is a proper lawful reason for processing (using) the data.

Fairness and transparency - processing (using) the data in a way that is fair and making sure that people understand how and why we are using it.

Purpose limitation – only using data for the legitimate reasons we originally collected it for.

Data minimisation – only collecting as much data as is needed and no more, not asking people to give unnecessary information for example.

Accuracy – ensuring data is up to date and there are no errors, or errors are corrected without delay.

Storage limitation – not keeping data for longer than is necessary

Integrity and confidentiality (security) – keeping people's data safe.

Accountability – being accountable for how we use data and how we comply with the above principles.

<u>These principles give the legal conditions that must be met when obtaining, handling, processing, transporting and storing personal data and are very important in the GDPR.</u>

Keeping to the spirit of these key principles is important for good data protection practice and compliance with the law. DMNW fully supports and follows these principles. Employees and any others who obtain, handle, process, transport and store personal data for DMNW must follow these principles. DMNW will provide training to our staff and volunteers on data protection and information security, this takes place on induction and then annually as part of our mandatory training programme.

Data protection lead

DMNW is currently not legally required to have a Data Protection Officer. However, a Data Protection Lead (see details below) has been identified and will be responsible for ensuring that the policy is implemented and will have the responsibility:

- To inform and advise the organisation, the board, and its employees about their obligations to comply with Data Protection Legislation.
- To monitor compliance with Data Protection Legislation, including managing internal data protection activities, and advise on data protection.
- Impact assessments: train staff and conduct internal audits.

- To ensure the Charity continues to be registered with the Information Commissioner and that our details remain up to date.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, service users, members etc).
- Staff and Volunteers are actively encouraged and supported through training and their line manager to report any concerns that they may have to improve both our data protection and services to users.

However, all staff and volunteers are also aware that a deliberate breach of the rules and procedures identified in this policy may result in disciplinary action being taken against them. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to legislation. In case of any queries or questions in relation to this policy please contact

DMNW's Data Protection Lead:

Gemma Gaskell Chief Executive Officer

Diversity Matters North West

20 Great Norbury Street, Hyde SK14 1BR

gemma@diversitymattersnw.org.uk

0161 368 3268

DMNW ensures that our details are registered with the Information Commissioner. The current certificate expires on 7th August each year. A copy of the notification is located in DMNW office. You can see the registration online on the Data Protection Register by going to https://ico.org.uk/ESDWebPages/Entry/ZA008032

Data collection

DMNW will only collect data that is 'necessary' to deliver our services and contracts. It will identify the lawful basis for processing data and ensure that this is communicated clearly within its privacy notices and that appropriate documentation of our data processing activities is recorded. When collecting data, DMNW will ensure that the individual:

- Clearly understands why the information is needed
- Understands what it will be used for and what will happen if they decide they do not want their information to be used (processed) in this way
- Where necessary, grants explicit consent, either written or verbal for data to be processed.
- Is, as far as reasonably practicable, able to understand what processing would require and able to give consent where necessary.
- Has received sufficient information on why their data is needed and how it will be used.

Further information on the data we collect including how we do this and why can be found in DMNW's Privacy Policy. There is a copy of this on our website.

Data Storage retention and disposal

Personal Information and records relating to DMNW's business and service delivery will be stored securely and will only be accessible to authorised staff and volunteers. Information will be stored for only as long as it is needed or required by law and will be disposed of appropriately.

The retention period for relevant data is recorded in DMNW's Record Keeping Policy and Procedure

DMNW will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure. The measures taken include:

- Personal Data will be kept in locked filing cabinets with access restricted to those people who have authority to access the data
- Password protection on personal information files
- Restricted access to computer files, drives and systems.
- Restricted access to People Cloud HR Platform
- Use of secure VPN mechanisms to ensure personal data does not need to be duplicated unnecessarily
- Data, including personal data, is backed up daily and information kept off site using secure cloud services
- Suitable encrypted attachments for sensitive personal information sent by email

Any deliberate unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

The Board are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.

Any deliberate unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

It is DMNW's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party. Any external destruction of data will be undertaken under contract to any relevant British Standard.

Accuracy of data and keeping data up to date

DMNW will ensure that all personal data collected and processed is kept accurate and up to date. The accuracy of data will be checked when it is collected and at regular intervals afterwards. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Training

All staff training on induction and annually.

All volunteers are made aware of GDPR regulations on induction and upon receipt of any new roles within the organisation.

DMNW will display information around the building to remind staff and volunteers of the principles of data protection.

This will be in the form of simple does and don'ts. Staff and volunteers will be reminded of their responsibilities at team meetings and in line management / supervision. Where required staff and volunteers will be offered additional training as part of training and professional development opportunities.

Data protection by design

DMNW is committed to considering data protection and privacy issues in everything we do. DMNW is committed to integrating data protection into all our activities and practices, from the design stage right through our delivery. This includes:

- Anticipating risk and invasions to privacy through the organisational risk register and taking steps to prevent harm to individuals.
- Considering data protection issues as part of the planning, design and implementation of systems, projects, services and delivery. Both through broader tools and Data Protection Impact Assessments as required.
- Only processing the personal data that we need for our purposes(s) and making sure that we only use the data for those purposes.
- Providing the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- Ensuring that any data processors we may use can provide sufficient guarantees of the measures they use for data protection.

Individual Rights

Right to be informed: Individuals have the right to be told how their personal data is collected, used, stored, and shared — at the time of collection and in clear, accessible language.

Example: When a South Asian woman registers for a domestic abuse support session, the charity provides her with a privacy notice explaining:

- *What data will be collected (e.g., name, contact, background information)*
- *Why it is being collected (e.g., to provide support and ensure safety)*
- *Who it may be shared with (e.g., healthcare or safeguarding partners, if necessary)*
- *How long it will be kept*
- *Her data rights*

The charity must make this information available upfront, ideally in writing (e.g., printed leaflet, welcome pack, or online), and explain it verbally if needed — especially where language or literacy may be a barrier.

Right to Access: Individuals have the right to know what personal data we hold about them.

Example: A woman who attended a health awareness workshop asks for a copy of all data you hold about her, including notes from her initial consultation and services used.

A copy of their data must be provided within one month.

Right to Rectification: Individuals can ask for their data to be corrected it if is inaccurate or incomplete.

Example: A service user notices their name is misspelled and their preferred language is wrong in your records. They ask you to correct it.

Errors must be correctly promptly, and the service user must be made aware that these changes have been made.

Right to Erasure ("Right to Be Forgotten"): Individuals can ask for their data to be deleted when there's no legal reason to keep it.

Example: A woman who previously accessed a training programme asks you to delete her records for safety and privacy reasons.

If there's no safeguarding or legal obligation to keep the data, you must erase it.

Right to restrict processing: Individuals can ask to pause or limit how their data is used in certain situations

Example: A service user asks that their data not be shared with partner organisation or used in case studies, even anonymously

We must stop or limit processing until the issue is resolved

Right to Data Portability: Individuals can request their data in a format that allows them to transfer it elsewhere.
Example: A bereavement support client moves to another city and asks for her records to be sent to a new support service.
Data should be provided in a readable, structured format like PDF or spreadsheet.

Right to Object: Individuals can object to their data being used in certain ways, like for marketing.
Example:
A training attendee receives emails about future sessions but doesn't want any more promotional messages.

We must stop using their data for this purpose immediately.

Rights in Relation to Automated Decision-Making and Profiling: People can challenge decisions made only by automated systems.
Example:
A client is referred by an online questionnaire to one type of service, but she disagrees and wants a staff member to review her case.

We must offer a human review of the decision and explain how it was made.

Disclosure and data sharing

DMNW may need to share data with other agencies such as local authorities, funding bodies and other community and voluntary agencies as part of its work. The individual will be made aware in most circumstances how and with whom their information will be shared as part of the Privacy Notice process.

However, there are some limited circumstances (where legislation allows) in which DMNW may disclose data (including sensitive data) without the individuals knowledge. These include:

- When required to by law – This may be as simple as providing information to HMRC for tax purposes.
- Protecting vital interests of an individual or other person – This includes safeguarding concerns where an individual may be at risk or in cases of medical emergencies. Sharing information for safeguarding purposes is now a recognised legitimate interest under the Data Use and Access Act 2025.
- The Data Subject has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights

DMNW regards the lawful and correct treatment of personal information as especially important to successful working, and to maintaining the confidence of those with whom we deal.

DMNW will ensure that personal information is treated lawfully and correctly. Staff or Volunteers who are unsure about whether they can legitimately disclose personal data to an individual or organisation should seek advice from their line manager or the Data Protection Lead.

Organisational Measures

DMNW will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, volunteers, contractors, or anyone else working on behalf of DMNW will be made fully aware of both their individual responsibilities and DMNW's responsibilities under the legislation and under this Policy and will be given a copy of this Policy. They will be asked to sign to confirm they have read, understood and will follow the policy.
- Only employees, volunteers, sub-contractors, working on behalf of DMNW that need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by DMNW.
- All employees, volunteers, contractors, working on behalf of DMNW handling personal data will be appropriately trained to do so.
- All employees, volunteers, contractors, working on behalf of DMNW handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

- The performance of those employees, volunteers, contractors, working on behalf of DMNW handling personal data shall be regularly evaluated and reviewed.
- All contractors, working on behalf of DMNW handling personal data will be issued with a contract containing the appropriate standard clauses relating to data protection and data processing as set out in GDPR legislation.
- A Data Protection Impact Assessment will be completed by staff with oversight and approval by the DPL should there be any sharing of personal data with any third parties.

Risk Management

The consequences of a personal data breach can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. This policy and the supporting policies and procedures are designed to minimise the risks and to ensure that the reputation of DMNW is not damaged through inappropriate or unauthorised access and sharing.

Data Protection is everyone's responsibility if staff or volunteers know or suspect that a personal data breach has occurred, then they should immediately contact the Data Protection Lead Gemma Gaskell.

DMNW makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of how personal data incidents might occur include through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g., email sent to the incorrect recipient)
- Human error
- Hacking attack

In the event of a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, DMNW will promptly assess the risk to individuals concerned and if appropriate report this breach to the ICO (more information is available on the ICO website). If a reportable breach has occurred DMNW is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it. In some cases, there may be a requirement to report to funders and the Charity Commission.

Staff and Volunteers are actively encouraged to report any incidents or concerns that they may have, to improve both our data protection and services to users. Staff and volunteers are also aware that they can be personally liable if they deliberately or maliciously use service user's personal data inappropriately. DMNW have a detailed Personal Data Breach Response Plan to guide managers in addressing any breaches that do occur.

Complaints
For complaints relating to data protection, please refer to our electronic complaints form, which can be found on our website and DMNW Complaints policy for information on the process and timescales, this can also be found on our website.

Responsibilities
The Board
The Board of trustees have overall responsibility to ensure that DMNW takes GDPR seriously.

Chief Executive Officers
The Chief Officers have lead responsibility for implementing and monitoring this policy

Employees
All employees are responsible for understanding and applying the GDPR Policy in their work, both individually and collectively.

Review Details
This policy was adopted in 2025 and will be reviewed every 5 years by the Board of Trustees, or earlier should legislation or circumstances demand.

Related Policies
- Data Breach
- Record Keeping
- Complaints
- Privacy Notice

Appendices
Appendix 1: Data Protection Impact Assessment Form

Diversity Matters North West

Data Protection Impact Assessment

What is a DPIA

A DPIA is a process designed to help organisations identify and minimize the data protection risks of a project or activity. It's a key part of the UK GDPR and other global data protection regulations, especially when processing personal data that could result in a high risk to individuals' rights and freedoms.

Who decided when a DPIA should take place

DMNW Data Protection Lead will ensure that DPIA's are completed when necessary and proportionate.

When is a DPIA required

Under UK GDPR, a DPIA is mandatory when:

- Using new technologies.
- Processing data on a large scale.
- Profiling individuals.
- Monitoring publicly accessible areas.
- Processing sensitive data (e.g., health, biometric).

Project Name	
Date	
Assessment Completed by	
Summary of why a DPIA is being completed	
Description of Processing	
Purpose of Processing	
Nature of Processing	
Type of Data	
Data Subjects	
Necessity and Proportionality	
Legal Basis for[2] Processing	
Data Minimisation	
Access Controls	

[2] A guide to lawful basis | ICO

Risk Assessment			
Risk Identified	Likelihood (Low, Med, High)	Impact (Low, Med, High)	Mitigation Measures

Measures to Address Risk	
Consultation	
Conclusion	