Disability Equality NW General Data Protection Rules (GDPR) Policy

---

Disability Equality NW - Data Protection Policy (2026 Edition)

(Fully updated to reflect UK GDPR, Data Protection Act 2018, ICO guidance 2024-2026)

---

1. Introduction

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 govern how Disability Equality NW (DENW) collects, uses, stores, shares, and disposes of personal data. DENW is committed to full compliance with all legal requirements and to maintaining the trust and confidence of clients, volunteers, staff, trustees, contractors, and partner organisations.

DENW processes personal data to deliver services effectively, meet contractual and legal obligations, and support organisational operations. All personal data will be handled securely, lawfully, fairly, and transparently, whether stored electronically, on paper, or by other means.

---

2. Data Protection Principles

DENW adheres to the six legally enforceable principles of UK GDPR. Personal data must be:

1. **Lawfulness, fairness, transparency**
   Processed lawfully, fairly, and in a transparent manner.
2. **Purpose limitation**
   Collected for specified, explicit, and legitimate purposes and not used in ways incompatible with those purposes.
3. **Data minimisation**
   Adequate, relevant, and limited to what is necessary.
4. **Accuracy**
   Accurate and kept up to date. Inaccurate data must be corrected or erased without delay.
5. **Storage limitation**
   Kept no longer than necessary, in line with DENW's retention schedule.
6. **Integrity and confidentiality**
   Processed securely, protecting against unauthorised access, unlawful processing, accidental loss, destruction, or damage.

---

3. Lawful Bases for Processing

DENW processes personal data under one or more lawful bases:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data (e.g., disability information) is processed under:

- Explicit consent
- Employment obligations
- Provision of health or social care
- Substantial public interest (e.g., safeguarding, equality monitoring)

4. Rights of Individuals

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (subject to legal exemptions)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making

DENW will respond to all valid requests in line with our Data Protection Complaints Policy.

Reasonable adjustments will be made for disabled individuals, including accepting verbal requests and providing information in accessible formats (e.g., large print, audio, Braille) where available.

---

5. Roles and Responsibilities

5.1 Data Protection Lead

DENW's CEO acts as the **Data Protection Lead**, responsible for:

- Overseeing compliance
- Maintaining policies
- Managing subject access requests
- Reporting data breaches
- Ensuring staff training
- Approving unusual disclosures

5.2 Staff, Volunteers (including Student Placements), Trustees

All personnel must:

- Follow this policy
- Complete mandatory data protection training
- Report any suspected breach immediately
- Ensure data accuracy
- Use secure systems and approved processes only

---

6. Data Collection and Use

DENW will:

- Collect only data necessary for service delivery or legal obligations
- Inform individuals how their data will be used
- Use data only for the purposes stated at collection
- Keep data accurate and up to date
- Review data regularly
- Delete or anonymise data when no longer required
- Ensure individuals can exercise their rights easily

---

7. Data Storage and Security

7.1 Electronic Data

Access requires individual logins and passwords for:

- Network drives
- Secure email
- Case management systems (AdvicePro)
- Volunteer and client databases
- Internal Wi-Fi (segregated for staff and visitors)

Security measures include:

- Multi-factor authentication (MFA)
- Encrypted devices
- Automatic screen-locking
- Password complexity and rotation
- Immediate revocation of access when staff leave
- Prohibition of shared accounts

7.2 Paper Records

- Stored in locked cabinets or secure rooms
- Digitised and originals destroyed unless legally required
- Never left unattended or visible to unauthorised individuals

7.3 Home Working

Staff working remotely must:

- Use encrypted devices
- Ensure secure Wi-Fi
- Prevent family/third-party access
- Dispose of printed documents securely
- Follow workstation security rules

---

8. Data Sharing

DENW will not share personal data with third parties unless:

- Consent has been obtained
- Required by law
- Necessary to protect vital interests
- Required for safeguarding
- Necessary for contracted service delivery

All third-party processors must have GDPR-compliant contracts.

---

9. Data Retention

DENW maintains a **Retention Schedule** specifying how long each category of data is kept. Examples:

- Client case records: 6 years
- Volunteer records: duration of involvement + 3 years
- HR files: 6 years after employment ends
- Financial records: 6 years
- Membership data: active membership + 2 years
- Emails: dependent on subject matter 6 months to 6 years

Data is securely destroyed when retention periods expire.

---

10. Subject Access Requests (SARs)

Requests must be made to the CEO (Data Protection Lead). DENW will:

- Verify identity
- Respond within 30 days
- Provide data in accessible formats
- Document verbal requests where needed
- Explain any lawful exemptions

---

11. Data Protection Impact Assessments (DPIAs)

DPIAs are required for:

- Case management systems
- Processing vulnerable individuals' data
- New technologies

- Large-scale special category data
- Supported Banking services
- Safeguarding-related processing

DPIAs must be completed before processing begins and reviewed at Team Meetings.

---

12. Training

All staff, volunteers, and trustees must complete:

- Induction GDPR training
- Annual refresher training
- Additional training when policies change

Significant breaches may result in disciplinary action.

---

13. Data Breach Reporting

A data breach includes loss, unauthorised access, accidental disclosure, or corruption of personal data.

DENW will:

- Require staff to report breaches **immediately** to the CEO
- Record all breaches
- Assess risk to individuals
- Notify the ICO within **72 hours** if the breach is likely to result in risk to individuals
- Notify affected individuals where required
- Take corrective action to prevent recurrence

DENW's ICO registration number: **Z8950065**

---

14. Privacy Notice

DENW will maintain an up-to-date Privacy Notice explaining:

- What data is collected
- Why it is collected
- How long it is kept
- How it is shared
- Individual rights
- Contact details for the Data Protection Lead

The Privacy Notice will be available online and in accessible formats.

---

15. Related Policies

- Confidentiality Policy
- Lone/Home Working Policy
- Acceptable Use (Internet & Email)
- Information Security Policy
- Retention Schedule
- Data Protection Complaints Policy

---

16. Review

This policy will be reviewed regularly, at least every three years or sooner if legislation or ICO guidance changes.
