DORSET WOMEN CIC
DATA PROTECTION & PRIVACY POLICY

Version 1.0
Approved by the Board: 18/05/2026
Review Date: Annual

---

1. Policy Statement

Dorset Women CIC is committed to protecting personal data and respecting the privacy of all individuals who engage with our work.

We process personal data lawfully, fairly and transparently in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR) (where applicable)

This policy applies to Directors, volunteers, contractors, partners and anyone acting on behalf of Dorset Women CIC.

---

2. Scope

This policy covers personal data relating to:

- Participants and event attendees
- Supporters and subscribers
- Volunteers and Directors
- Partners and stakeholders
- Funders and donors

It applies to all formats of data, including:

- Digital files
- Email correspondence
- Cloud-based systems
- Paper records
- Audio or video recordings

3. Data Protection Principles

Dorset Women CIC will ensure that personal data is:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Retained only for as long as necessary
6. Processed securely
7. Accountable and demonstrably compliant

---

4. Lawful Basis for Processing

We rely on one or more of the following lawful bases:

4.1 Consent

Where individuals opt in to receive communications, newsletters or marketing.

4.2 Legitimate Interests

To:

- Deliver community events
- Manage relationships with stakeholders
- Promote Dorset Women CIC activities
- Monitor participation and impact

Legitimate interest assessments will be conducted where required.

4.3 Contractual Necessity

Where processing is required to fulfil an agreement.

4.4 Legal Obligation

For statutory reporting and financial record-keeping.

---

5. Special Category Data

Due to the nature of our work supporting and amplifying women's voices, we may collect limited special category data, including:

- Ethnicity
- Disability
- Gender identity
- Socioeconomic background

This data will only be processed:

- With explicit consent, or
- Where necessary for substantial public interest purposes

Such data will be subject to enhanced security controls.

---

6. Data We Collect

Depending on engagement, this may include:

- Name and contact details
- Demographic information (optional)
- Event registration information
- Feedback responses
- Media consent records
- Donation records
- Volunteer role information

We do not knowingly collect unnecessary personal data.

---

7. How We Use Personal Data

We use personal data to:

- Deliver events and programmes
- Communicate updates and opportunities

- Meet safeguarding obligations
- Monitor reach and impact
- Meet funder reporting requirements
- Comply with legal and regulatory duties

We do not sell personal data.

---

8. Data Sharing

We may share personal data only where necessary:

- With event venues (e.g. accessibility requirements)
- With trusted service providers (e.g. email platforms)
- With statutory authorities (where safeguarding requires)
- With regulators (where legally required)

All third-party providers must demonstrate appropriate data protection standards.

---

9. Data Retention

Personal data will be retained only as long as necessary.

Indicative retention periods:

- Event attendance data: 2 years
- Volunteer records: duration of involvement + 3 years
- Financial and donation records: 7 years
- Safeguarding records: minimum 7 years (or longer if required)
- Complaints records: 6 years

After this period, data will be securely deleted or anonymised.

---

10. Data Security

We implement appropriate technical and organisational measures, including:

- Secure cloud-based storage

- Password-protected systems
- Two-factor authentication where possible
- Restricted access on a need-to-know basis
- Regular review of permissions

Paper records, where used, will be stored securely.

---

11. Data Breach Procedure

A personal data breach includes:

- Unauthorised access
- Accidental disclosure
- Loss of devices or files

If a breach occurs:

1. It must be reported immediately to the designated Data Protection Lead.
2. The breach will be assessed within 24 hours.
3. Where required, the ICO will be notified within 72 hours.
4. Affected individuals will be informed where appropriate.

All breaches will be recorded in a breach log.

Where a breach constitutes a serious incident, it will be handled under the Serious Incident Reporting Framework.

---

12. Individual Rights

Individuals have the right to:

- Access their personal data
- Request correction
- Request erasure (where applicable)
- Restrict processing
- Object to processing

- Withdraw consent
- Data portability (where applicable)

Requests must be responded to within one calendar month.

---

13. Marketing & Communications

We will:

- Obtain consent before sending electronic marketing communications
- Provide clear opt-out mechanisms
- Honour unsubscribe requests promptly

---

14. Confidentiality

All Directors, volunteers and contractors must:

- Maintain confidentiality
- Only access data necessary for their role
- Not disclose personal data without authorisation

Breaches of confidentiality may result in removal from their role.

---

15. Children and Vulnerable Adults

Where Dorset Women CIC engages with children or vulnerable adults:

- Safeguarding policy will take precedence
- Additional care will be taken in handling personal data
- Parental/guardian consent will be obtained where required

---

16. Governance and Oversight

The Board retains ultimate accountability for data protection compliance.

A named Director will act as Data Protection Lead and will:

- Maintain data inventory

- Oversee breach response
- Ensure annual review
- Report significant risks to the Board

---

17. Complaints About Data Protection

If an individual is unhappy with how we handle their data, they may:

1. Contact Dorset Women CIC directly.
2. Escalate to the Information Commissioner's Office (ICO) if unsatisfied.

ICO Website: www.ico.org.uk

---

18. Policy Review

This policy will be reviewed annually or sooner if:

- Legislation changes
- A serious incident occurs
- Organisational structure changes