

GDPR Policy & Privacy Notice

The Woodland Warrior Programme CIC &
Hidden Valley Bushcraft Ltd

Version 3	Date 20/1/26
Review Date	20/01/27
Signed	<i>L Goldsmith</i>



1. Introduction

The Woodland Warrior Programme (WWP) is run in partnership with Hidden Valley Bushcraft Ltd (HVB) For the purpose of this policy 'we' refers to WWP and HVB.

This GDPR Policy outlines how **The WWP and HVB** ("we", "our", "the organisation") collects, uses, stores, and protects personal data, including special category data relating to health. We are committed to safeguarding the privacy and rights of the individuals we support, our staff, volunteers, and partners, in accordance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- Relevant guidance from the Information Commissioner's Office (ICO)
-

Because we work with individuals who may have or be experiencing a mental or physical health condition, we recognise the heightened sensitivity of the data we handle and apply the highest standards of confidentiality and security.

2. Scope

This policy applies to:

- All employees, volunteers, contractors, and partners who process personal data on behalf of the organisation.
- All personal data relating to service users, including special category (sensitive) data such as health information.

3. Lawful Bases for Processing

We process personal data only when a lawful basis under Article 6 of the UK GDPR applies. For most health-related data, our lawful bases include:

3.1 Article 6 Lawful Bases

- **Consent** – freely given, informed, and specific permission from the individual.
- **Contract** – where processing is necessary for delivering agreed services.
- **Legal Obligation** – e.g., safeguarding or reporting requirements.
- **Vital Interests** – to protect someone's life in an emergency.
- **Legitimate Interests** – when processing is necessary for our operations and does not override the rights of the individual.

3.2 Article 9 Special Category Data Conditions

Because we process health data, we rely on one or more of the following:

- **Explicit Consent**
- **Vital Interests** where the individual is incapable of giving consent
- **Substantial Public Interest**, such as safeguarding of vulnerable individuals

4. Types of Personal Data We Collect

We collect and process:

4.1 Personal Data

- Name, date of birth, address, contact details
- Emergency contacts

4.2 Special Category (Sensitive) Data

- Mental and physical health information
- Medication details where applicable

This information will be collected from applicants as part of the application form. Explicit consent is required to obtain this data.

5. How We Use Personal Data

We use personal data to:

- Support beneficiaries well-being throughout the programme
- Provide therapeutic activities to support mental and physical health
- Maintain accurate records of support provided
- Manage safeguarding or risk concerns
- Contact the named person in case of an emergency
- Communicate with beneficiaries and relevant professionals including news, events, additional courses as well as signposting to services and information.

6. Data Sharing

We may share personal data with:

- NHS mental health teams
- GPs and healthcare providers
- Social services
- Emergency services
- Safeguarding authorities

Data is shared only when necessary, proportionate, and lawful. We always aim to inform individuals unless doing so would increase risk of harm.

7. Data Security

We maintain strict data protection measures, including:

- Password-protected and encrypted digital systems
- Secure storage for paper files
- Role-based access controls
- Regular staff training on confidentiality and safeguarding
- Reporting and investigating any data breaches in line with ICO requirements

8. Data Retention

We retain data only for as long as necessary and in line with our retention schedule:

- General beneficiary records: **upon exiting** the programme
- Safeguarding records: **75 years** after exiting the programme
- Staff and volunteer records: **6 years** after employment ends

After retention periods, information is securely destroyed.

9. Individual Rights

Under GDPR, individuals have the right to:

- Access their data (Subject Access Request)
- Request correction of inaccurate information
- Request erasure (“right to be forgotten”)
- Restrict processing
- Object to processing
- Data portability (where applicable)
- Withdraw consent at any time
- Lodge complaints with the **Information Commissioner’s Office (ICO)**

Requests are handled within **one month**.

10. Data Protection Officer (DPO) / Responsible Person

Louise Goldsmith acts as our Data Protection Officer or Data Protection Lead.

Contact: woodlandwarriorprogramme@outlook.com

11. Data Breach Procedure

Any suspected data breach must be reported immediately to the DPO. We will:

- Investigate promptly
- Mitigate any risks
- Notify the ICO within **72 hours** if the breach risks harm
- Inform affected individuals when necessary

11.1 Record-Keeping

All data breaches—whether reported to the ICO or not—are recorded in the **Data Breach Register**, including:

- Date and time of the incident
- Nature of the breach
- Type of data involved
- Individuals affected
- Likely consequences
- Actions taken to contain and recover
- Notification decisions
- Lessons learned

Records are retained for a minimum of **6 years**.

11.2 Review and Prevention

Following a breach, we will:

- Conduct a full internal review
- Identify root causes
- Implement improvements (e.g., training, technical controls, revised procedures)
- Update risk assessments and policies if required

12. Policy Review

This policy is reviewed annually or sooner if legislation changes or services evolve.

Last reviewed: 20th January 2026

Next review due: 20th January 2027