Thriveology Wellness CIC

Data Protection Policy.

September 2026

DATA PROTECTION POLICY

September 2026

INTRODUCTION

Our Data Protection Policy outlines Thriveology's commitment to protecting the confidentiality, integrity, and availability of personal data in compliance with applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR) and other relevant local laws.

This policy applies to all employees, volunteers, and third-party service providers who handle personal data on behalf of Thriveology. It covers all data collected and processed by the organisation, regardless of the format in which it exists (electronic or paper).

DEFINITIONS

Personal Data: Any information relating to an identified or identifiable individual.

Data Subject: An individual whose personal data is processed by the organisation.

Processing: Any operation or set of operations performed on personal data, including collection, storage, use, and dissemination.

DATA PROTECTION PRINCIPLES

Thriveology is committed to ensuring that personal data is:

1. Lawful, Fair, and Transparent: Processing personal data in a lawful manner, ensuring fairness and transparency.
2. Purpose Limitation: Collecting personal data only for specified, legitimate purposes and not further processing it in a manner incompatible with those purposes.
3. Data Minimisation: Collecting only personal data that is necessary for the purposes of processing.

4. Accuracy: Taking reasonable steps to ensure that personal data is accurate and up to date.
5. Storage Limitation: Retaining personal data only as long as necessary for the purposes for which it was collected.
6. Integrity and Confidentiality: Ensuring appropriate security measures are in place to protect personal data against unauthorised access, loss, or damage.

ROLES AND REPSONSIBILITIES

Data Protection Officer (DPO): The DPO is responsible for overseeing data protection compliance, serving as the point of contact for data subjects and regulatory authorities, and ensuring that data protection policies and procedures are implemented.

Employees and Volunteers: All employees and volunteers are responsible for handling personal data in accordance with this policy and reporting any data breaches or suspected breaches to the DPO immediately.

DATA SECURITY

Thriveology will implement appropriate technical and organisational measures to protect personal data from unauthorised access, alteration, disclosure, or destruction. These measures include:

- Encryption of sensitive data.

- Secure access controls and authentication mechanisms.

- Regular security assessments and audits.

- Training on data protection and security awareness.

DATA BREACH RESPONSE

In the event of a data breach, Thriveology will:

1. Implement a response plan to contain and assess the breach.
2. Notify affected data subjects and relevant regulatory authorities as required by law.

3. Document the breach and the response actions taken.

DATA SUBJECT RIGHTS

Data subjects have the following rights concerning their personal data:

- Right to Access: The right to request access to their personal data held by the organisation.
- Right to Rectification: The right to request correction of inaccurate or incomplete personal data.
- Right to Erasure: The right to request deletion of their personal data under certain circumstances.
- Right to Restrict Processing: The right to request the restriction of processing of their personal data under certain conditions.
- Right to Data Portability: The right to request the transfer of their personal data to another organisation in a structured, commonly used format.
- Right to Object: The right to object to the processing of their personal data under certain conditions.

TRAINING AND AWARENESS

Thriveology will provide regular training and awareness programmes to employees and volunteers regarding data protection responsibilities and best practices.

POLICY REVIEW

This Data Protection Policy will be reviewed annually and updated as necessary to ensure compliance with applicable laws and regulations and to reflect changes in organisational practices.

ACKNOWLEDGMENT

By handling personal data on behalf of Thriveology, all employees, volunteers and third-party service providers acknowledge that they have read, understood, and agree to comply with this Data Protection Policy.

CONTACT INFORMATION

For questions or concerns regarding this policy, please contact our Data Protection Officer; Mrs Kerry Wakor at kerry@thriveology.co.uk.

Review Date: SEPT 2027

APPENDIX: POST-16 DATA PROCESSING & PRIVACY

Purpose of This Appendix

This appendix outlines how Thriveology Wellness CIC processes, stores, and shares personal data relating to Post-16 young people participating in our workplace-readiness, life-skills, and supported employment programmes. It should be read alongside the main Data Protection Policy (September 2026).

1. Categories of Data Processed for Post-16 Young People

To deliver safe, effective Post-16 provision, Thriveology may collect and process the following personal data:

- **Identification information:** name, date of birth, contact details

- **Educational and SEND information:** EHCP outcomes, learning needs, support plans
- **Vocational and workplace-readiness data:** skills assessments, vocational profiles, placement suitability notes
- **Life-skills and independence data:** travel-training progress, community-based learning records, independent-living development
- **Health or safeguarding information:** only where necessary to ensure safety during off-site activities or employer placements
- **Emergency contact details:** for use during workplace activities, travel training, or community sessions

All data is processed in accordance with GDPR principles, including data minimisation and purpose limitation (e.g., “Collecting only personal data that is necessary for the purposes of processing”).

2. Purposes of Processing

Personal data for Post-16 learners is processed to:

- Support transition into employment, apprenticeships, or further education
- Deliver workplace-readiness coaching, vocational activities, and life-skills teaching
- Ensure safety during off-site learning, employer placements, and travel training
- Communicate with families, carers, employers, and external agencies
- Meet statutory safeguarding, SEND, and duty-of-care requirements
- Monitor progress against EHCP outcomes and programme goals

3. Lawful Basis for Processing

Thriveology processes Post-16 learner data under the following lawful bases:

- **Public Task:** delivering education, training, and SEND-related provision
- **Legitimate Interests:** ensuring safe participation in workplace and community activities
- **Legal Obligation:** safeguarding, reporting requirements, and compliance with SEND legislation
- **Consent:** where optional activities require additional data sharing (e.g., employer photographs, publicity materials)

4. Data Sharing for Post-16 Provision

Where necessary and proportionate, Thriveology may share Post-16 learner data with:

- Employers offering work experience or supported placements
- Training providers, vocational partners, and community organisations
- Local authorities, SEND teams, and social care professionals
- Transport providers involved in travel training
- External agencies supporting employment or independent-living development

All sharing is strictly controlled, documented, and compliant with GDPR transparency requirements (e.g., “Processing personal data in a lawful manner, ensuring fairness and transparency”).

5. Additional Safeguards for Post-16 Data

Thriveology applies enhanced safeguards to Post-16 data, including:

- Secure handling of employer-related documentation
- Controlled access to vocational profiles and workplace assessments
- Safe storage of travel-training routes, risk assessments, and off-site activity plans
- Staff training specific to Post-16 data handling and workplace-readiness activities

These measures complement the organisation's existing security commitments (e.g., "Encryption of sensitive data" and "Secure access controls").

6. Rights of Post-16 Young People

Post-16 learners have full GDPR rights, including:

- Right of access
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object

Where a young person requires support to exercise these rights, Thriveology will work with parents, carers, or authorised representatives.

7. Retention of Post-16 Data

Post-16 learner data is retained only for as long as necessary to fulfil the purposes for which it was collected, in line with Thriveology's retention schedule and GDPR storage-limitation principles (e.g., "Retaining personal data only as long as necessary").

8. Contact Information

For questions or concerns regarding Post-16 data processing, please contact:

Data Protection Officer: Mrs Kerry Wakor kerry@thriveology.co.uk