



Horserenity CIC

Data Protection Policy

Date of Issue: 2nd December 2025

Review Date: 1st December 2026

Produced by Dan Vivian

Reviewed by Sarah Vivian

1. Introduction

Horserenity CIC (“the organisation”) is committed to protecting the privacy and security of all personal data it collects and processes. As an equine facilitated learning centre, we work with children, young people, and vulnerable adults, which requires heightened diligence, security, and accountability for all information handled.

This policy sets out how Horserenity CIC ensures compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, particularly regarding the safeguarding of young and vulnerable learners.

2. Purpose of the Policy

This policy aims to:

- Ensure lawful, fair, and transparent processing of personal data.
- Protect the rights and freedoms of all learners, especially children and young people.
- Ensure staff and volunteers understand their responsibilities in relation to data.
- Establish protocols for collecting, storing, sharing, and disposing of data.
- Demonstrate compliance with UK data protection law and sector-specific safeguarding requirements.

3. Scope

This policy applies to:

- Directors
- Employees
- Volunteers
- Contractors
- Anyone processing data on behalf of Horserenity CIC

It covers all forms of data processing, including electronic, paper-based, visual, audio, and digital media.

4. Definitions

Personal Data: Information that identifies an individual (e.g., name, address, contact details).

Special Category Data: Sensitive information requiring extra protection, including:

- Medical information
- Mental health data
- Safeguarding information
- Ethnicity, religion, or other sensitive characteristics

Processing: Any action performed on data, including collection, storage, sharing, or deletion.

Data Subject: The individual whose data is being processed.

Data Controller: Horserenity CIC—the organisation that determines the purpose and means of processing data.

Data Processor: Anyone acting on behalf of the organisation.

5. Data Protection Principles

Horserenity CIC adheres to the seven principles of the UK GDPR. Personal data must be:

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. Stored only as long as necessary
6. Processed securely
7. Demonstrated through accountability and documented compliance

6. Legal Basis for Processing Data

Horserenity CIC processes data under the following lawful bases:

6.1 Contract

For delivering equine-facilitated learning services and managing learner participation.

6.2 Legal Obligation

Meeting safeguarding, health and safety, charity governance, and regulatory requirements.

6.3 Vital Interests

To protect a learner's life or prevent serious harm, especially in emergencies.

6.4 Consent

When processing requires explicit permission, e.g.:

- Use of images
- Sharing updates with external professionals
- Communication beyond service delivery

6.5 Legitimate Interests

For operational management, security, service improvement, and welfare monitoring.

6.6 Special Category Conditions

When handling medical, behavioural, or safeguarding data, Horserenity CIC relies on:

- Explicit consent
- Safeguarding obligations
- Vital interests
- Support of social care services

7. Types of Data Collected

Horserenity CIC may collect:

7.1 Personal Data

- Name, date of birth, age
- Contact details
- Emergency contacts
- Education setting or care status

7.2 Special Category Data

- Medical and mental health information
- Medication details
- Allergies
- Risk assessments
- Behavioural and wellbeing information
- Safeguarding records

7.3 Session and Attendance Data

- Attendance records
- Session notes
- Progress reports

7.4 Digital Data

- Photographs or videos (with consent)
- Electronic communications
- CCTV footage (if used)

7.5 Staff/Volunteer Data

- Training records
- DBS checks
- Personnel files

8. Data Collection and Consent

Horserenity CIC will:

- Collect only the data required for safe and effective service delivery.
- Obtain informed consent from parents/carers for children under 13, or from learners 13+ where appropriate (in line with UK data protection guidance).
- Ensure consent is freely given, specific, informed, and revocable at any time.
- Maintain a clear record of consent forms.

Consent is *not* required for safeguarding or vital-interest processing.

9. Data Storage and Security

9.1 Physical Records

- Stored in locked, secure cabinets.
- Access limited to authorised staff only.

9.2 Digital Records

- Stored on secure password-protected systems.

- Encrypted where appropriate.
- Access managed via user permissions.

9.3 Transporting Data

- Sensitive data must not be taken offsite unless essential.
- Devices must be password-protected and encrypted.

9.4 Breach Prevention

- Staff must follow good cyber hygiene.
- Portable devices (phones, laptops) must have screen locks, PINs, and updates enabled.

10. Sharing and Disclosure of Data

Horserenity CIC may share data:

10.1 With Consent

- With schools, social workers, or other support agencies.
- For promotional materials (images/videos).

10.2 Without Consent

Only when legally justified:

- Safeguarding concerns
- Medical emergencies
- Court orders
- Police or local authority enquiries
- Serious risk to life or welfare

All sharing will be proportionate and documented.

11. Retention of Records

Horserenity CIC follows recommended retention schedules:

- **Safeguarding records:** Up to 25 years, or as advised by local authority
- **General learner records:** 7 years after final session
- **Accident/incident reports:** 3–40 years depending on case
- **Staff records:** 6 years post-employment
- **Financial data:** 7 years

Data is securely destroyed at the end of the retention period.

12. Rights of Data Subjects

Learners (or their guardians) have the right to:

- Be informed about how data is used
- Access their data (“subject access request”)
- Rectification of inaccurate data
- Erasure (where legal grounds allow)
- Restrict processing
- Object to processing
- Data portability (where applicable)

Requests must be made in writing and will be answered within **one month**.

13. Subject Access Requests (SARs)

- Requests must be verified to ensure identity.
- Responses will be completed within 30 days unless the request is complex.
- Information may be withheld if disclosure presents safeguarding risks or breaches legal obligations.

14. Data Breaches

A data breach includes loss, unauthorised access, or unlawful disclosure of data.

Horserenity CIC will:

- Contain the breach immediately.
- Notify the Data Protection Lead.
- Report notifiable breaches to the **Information Commissioner's Office (ICO)** within 72 hours.
- Inform affected individuals where there is a high risk to their rights and freedoms.
- Document all breaches, actions, and outcomes.

15. Training and Awareness

All staff and volunteers must:

- Complete data protection training during induction.
- Refresh training annually.
- Follow safeguarding, confidentiality, and digital security protocols.

Trustees will oversee compliance across the organisation.

16. Data Protection Lead

Horserenity CIC appoints a **Data Protection Lead (DPL)** responsible for:

- Monitoring compliance
- Acting as contact for data subjects
- Managing breaches
- Liaising with the ICO

Data Protection Lead:

Name/Role: Dan Vivian

Email: dan@horserenity.co.uk

Phone: 07887642428

17. Policy Review

This policy will be reviewed:

- Annually
- After major organisational changes
- After significant data incidents
- Following updates to legislation or ICO guidance

