Data Protection (GDPR) Policy

Neuro-Inclusive Hospitality CIC

May 2026

Document Owner: Corey Palmer
Next Review: May 2027

1. Introduction

Neuro-Inclusive Hospitality CIC ("NIH", "we") collects and uses personal data while delivering training, consultancy, e-learning, and community-interest activity. This policy explains how we comply with UK data protection law, principally the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and what people whose data we hold can expect from us.

Because much of our work involves people sharing whether they are neurodivergent, we are particularly careful with special category data relating to health and disability.

2. Who we are

Data Controller	Neuro-Inclusive Hospitality CIC
Company number	17106129
Registered office	10 Falsgrave, Scarborough, YO12 5AT
ICO registration	**ZC160829**
Data Protection Lead	Corey Palmer
Contact	Coreypalmer@nihcic.com

We are not currently required to appoint a statutory Data Protection Officer (DPO) under UK GDPR Article 37. The Director discharges the equivalent function and is the single point of contact for data protection enquiries.

3. Definitions

- **Personal data** is any information relating to an identified or identifiable living individual.
- **Special category data** personal data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data for identification, health, sex life, or sexual orientation. Information about neurodivergence is treated as health data.
- **Processing** anything we do with personal data: collecting, storing, using, sharing, and deleting.
- **The data subject** is the living individual the data relates to.

4. Our data protection principles

We commit to processing personal data in line with the six principles in UK GDPR Article 5:

1. Lawfulness, fairness, and transparency.
2. Purpose limitation collected for specified, explicit, legitimate purposes only.
3. Data minimisation adequate, relevant, and limited to what is necessary.
4. Accuracy kept accurate and up to date.

5. Storage limitation is kept no longer than necessary.
6. Integrity and confidentiality are protected by appropriate security.

We are also accountable for these principles, and can demonstrate compliance through the records, registers, and assessments referenced in this policy.

5. What personal data do we collect

From participants in our training

- Name, job title, organisation, contact details, accessibility requirements.
- Booking and attendance records, assessment results, and certificates.
- Where you choose to disclose it: information about your neurodivergence or disability.
- Images, video, or audio (only where you have signed our Consent Form and only for the purposes you ticked).

From client organisations

- Contact details of key contacts (HR, L&D, GM, Ops).
- Information about your organisation's neuroinclusion baseline, where you choose to share it for diagnostic or design purposes.

From visitors to our digital channels

- Contact details you submit through forms, the lead magnet, or e-learning sign-up.
- Analytics data from our website and CRM, including IP address, device, referrer, and engagement metrics.

From job applicants, associates, and contractors

- Information needed to engage, pay, and supervise you, including identity, qualifications, references, and (where required) DBS check status.

6. Lawful bases we rely on

We rely on the following UK GDPR Article 6 lawful bases:

- **Consent** for marketing, optional case studies, and images/video used externally.
- **Contract** to deliver training, consultancy, or e-learning, we have agreed to provide.
- **Legal obligation** for accounting, tax, employment, and CIC reporting requirements.
- **Legitimate interests** for course administration, internal analytics, and quality improvement (always balanced against your rights).

For special category data (including neurodivergence-related information), we rely additionally on Article 9 conditions, principally:

- **Explicit consent** Article 9(2)(a) wherever you choose to disclose neurodivergent identity in a way that is recorded.
- **Substantial public interest equality of opportunity or treatment** Article 9(2)(g) read with Data Protection Act 2018, Schedule 1, Part 2, paragraph 8, for monitoring purposes only.

7. How we use personal data

- To deliver, certify, and improve training, consultancy, and e-learning.
- To communicate with you about bookings, certificates, and (with consent) future opportunities.
- To meet our legal, regulatory, and CIC accountability obligations.
- To monitor equality, diversity, and inclusion outcomes in aggregate form.
- To investigate complaints, incidents, and safeguarding concerns.

8. Sharing your data

We share personal data only where necessary, and never sell it. Typical recipients are:

- Our cloud service providers (e.g. CRM, email, e-learning, file storage) are acting as data processors under a written contract.
- Accreditation bodies — limited to what is required to evidence training quality.
- Auditors, accountants, and legal advisers, under duties of confidence.
- Regulators (ICO, Companies House, HMRC, the CIC Regulator) where we are legally required to do so.
- Law enforcement, where lawful and proportionate.

9. International transfers

Some of our processors operate outside the UK. Where personal data is transferred internationally, we rely on UK adequacy regulations or appropriate safeguards (e.g. International Data Transfer Agreement, IDTA, or UK Addendum to the EU Standard Contractual Clauses), together with a transfer risk assessment. A list of our current processors and the safeguards in place is available on request.

10. How long do we keep data

Record type	Retention period
Booking and attendance records	6 years from the end of the course
Signed consent forms	6 years from the end of the course
Assessment results and certificates	6 years from issue
Anonymised case studies (where consented)	Until consent is withdrawn or no longer used
Images/video used externally (where consented)	Until consent is withdrawn or the marketing cycle ends, max 5 years
Complaints register	6 years from final response
Accounting and HMRC records	7 years from the end of the tax year
Employment/associate records	6 years from the end of the engagement
Marketing CRM contact (after unsubscribe)	Suppression list only no further use

Record type	Retention period
Website analytics	26 months (default Google Analytics 4)

11. Security

We take appropriate technical and organisational measures, proportionate to our scale and the risks involved, including:

- Access control on cloud systems with multi-factor authentication.
- Encryption in transit (TLS) and at rest for our primary cloud storage.
- Role-based access: staff and associates only see data they need.
- Confidentiality clauses in all associate and contractor agreements.
- Secure disposal of paper records via cross-cut shredding.
- Regular review of our data inventory and processor list.

12. Your rights

Under UK GDPR, you have the right to:

- be informed about how we use your data;
- access the personal data we hold about you (Subject Access Request);
- have inaccurate data corrected;
- ask for data to be erased, where the law allows;
- restrict our processing in certain circumstances;
- data portability, where the lawful basis is consent or contract;
- object to processing based on legitimate interests or for direct marketing;
- not be subject to a decision based solely on automated processing that has legal or similarly significant effects;
- withdraw consent at any time, where consent is the basis we rely on.

To exercise any of these rights, contact [Director Name] at [contact email]. We will respond within one calendar month. There is no fee for most requests.

13. Subject Access Requests

You can ask for a copy of the personal data we hold about you. We may need to verify your identity proportionately before responding. Where a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse it, and will explain our reasons and your right to complain.

14. Personal data breaches

If we discover, or are notified of, a personal data breach, we will:

7. Contain and assess the breach as quickly as possible.

8. Notify the ICO within 72 hours, where the breach is likely to risk individuals' rights and freedoms.
9. Notify affected individuals without undue delay, where the risk is high.
10. Record the breach in our internal breach register, regardless of whether external notification is required.
11. Review what happened, and update controls or training to reduce the chance of a repeat.

15. Cookies and analytics

Our website and e-learning platform use a limited set of cookies and similar technologies. Strictly necessary cookies are set without consent. Analytics and marketing cookies are set only after consent through our cookie banner, and you can change your preferences at any time. Full details are in our Cookie Notice.

16. Direct marketing

We send marketing emails only with consent or, in limited business-to-business contexts, on the soft opt-in basis permitted by PECR. Every marketing email contains a clear unsubscribe link, and we honour unsubscribes within 5 working days.

17. Children

Our training is designed for adult professionals. Where minors (16- and 17-year-old apprentices) attend a session, we obtain parental/guardian consent in addition to their own and apply enhanced data minimisation.

18. Roles and responsibilities

- **The Director** owns this policy, the data inventory, and the breach register, and is the primary point of contact for data subjects and the ICO.
- **Associate trainers and contractors** must process data strictly in line with this policy and their written agreement.
- **All NIH personnel** complete data protection awareness training on engagement and at least annually thereafter.

19. Concerns and complaints

If you are unhappy with how we have handled your personal data, please tell us first by emailing **coreypalmer@nihcic.com**. You can also complain to the Information Commissioner's Office at any time: ico.org.uk, 0303 123 1113, or in writing to Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

20. Review

This policy is reviewed at least every 12 months, and after any material change to our services, technology, or the law. Next review: 26 May 2027.

Authorisation

Name	Corey Palmer
Role	Director / Data Protection Lead, Neuro-Inclusive Hospitality CIC
Signature	C. Palmer
Date	06/06/2026