HUMANISE SOLUTIONS
Elevating People · Official Policy (Effective 1 January 2026)

Data Protection Policy

Version	Version 2.0
Effective date	1 January 2026
Next review date	1 January 2027
Approved by	Scott Ward (CEO)
Policy owner	CEO

Document control: This document is controlled. Printed copies may not be current. The latest approved version is held by Humanise Solutions. Changes are recorded in the version-control register and approved by the policy owner.

CITY & GUILDS ASSURED ALIGNMENT
Accurate, secure and well-governed personal data underpins our City & Guilds Assured provision. Learner records, management information and quality-assurance evidence provide the audit trail required to gain and maintain Assured endorsement, and are processed lawfully and securely throughout the learner journey.

1. Policy statement

Humanise Solutions Ltd ("Humanise Solutions", "we", "us") is committed to ensuring the privacy, security and lawful handling of all personal data we hold and process. We recognise that the people we work with – learners, employees, associates, partners and stakeholders – trust us with their information, and we are committed to honouring that trust by handling data transparently, ethically and securely at all times.

This policy sets out how we collect, record, store, use, share, retain and dispose of personal data, including data processed through the Humanise Solutions Digital Academy (our Learning Management System, "the LMS"). It explains our obligations, the rights of individuals, and the responsibilities of everyone who handles personal data on our behalf. It applies to personal data in any form, whether held electronically or on paper.

2. Purpose and objectives

The objectives of this policy are to:

- Ensure full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- Protect the rights and freedoms of data subjects, particularly learners and vulnerable individuals.
- Define clear accountability for data protection across the organisation.
- Ensure that data supporting our quality-assurance, City & Guilds Assured and funder-reporting obligations is accurate, secure and appropriately retained.
- Minimise the risk of data breaches and ensure an effective response where they occur.

3. Scope

This policy applies to all personal data processed by Humanise Solutions and to all those who process it on our behalf, including employees, contractors, associates, volunteers and delivery partners. It covers all of our services, including employment support, adult skills, leadership development, ESOL, coaching, wellbeing and digital learning, and all data processed via the Digital Academy. Delivery partners and processors must comply with this policy and with the terms of any data-processing agreement in place.

4. Legislative and regulatory framework

We process personal data in accordance with:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018.
- The Privacy and Electronic Communications Regulations (PECR) for electronic marketing.
- Relevant safeguarding, employment, equality and funding/contractual requirements that affect how data is processed and shared.

5. Definitions

Personal data	Any information relating to an identified or identifiable living individual.
Special category data	Sensitive data such as health, ethnicity, religion or sexual orientation, requiring additional protection.
Processing	Any operation performed on personal data, including collecting, recording, storing, using, sharing and deleting.
Data subject	The individual to whom the personal data relates.
Controller	The party that determines the purposes and means of processing (Humanise Solutions for its services).
Processor	A party that processes data on behalf of the controller (e.g. an LMS provider).

6. Data protection principles

We comply with the seven principles of the UK GDPR. Personal data must be:

- Processed lawfully, fairly and transparently – individuals are told who we are, what we do with their data and why.
- Collected for specified, explicit and legitimate purposes (purpose limitation).
- Adequate, relevant and limited to what is necessary (data minimisation).
- Accurate and, where necessary, kept up to date.
- Kept no longer than necessary (storage limitation).
- Processed securely, ensuring integrity and confidentiality.
- Handled in a way that we can demonstrate compliance (accountability).

7. Lawful bases for processing

We identify and record an appropriate lawful basis before processing personal data:

- Consent – for marketing communications and optional learner feedback, freely given and withdrawable at any time.
- Contract – for delivering training and services to clients and learners.
- Legal obligation – for safeguarding, health and safety, and statutory or funder reporting.
- Legitimate interests – for internal evaluation, quality assurance and service improvement, balanced against individuals' rights.

Where we process special category data (for example equality and diversity information or wellbeing notes), we identify an additional condition under Article 9, such as explicit consent, safeguarding, or reasons of substantial public interest, and apply appropriate safeguards.

8. Personal data we process

We only collect data that is necessary for specified purposes. Depending on the relationship, this may include:

- Identity and contact data: name, contact details and date of birth.
- Equality and diversity data (e.g. ethnicity, gender), processed to monitor inclusion and meet funder requirements.
- Background data: employment status, qualifications and learning history.
- Learning data: engagement, progress, achievement and completion records held in the Digital Academy.

- Wellbeing and support data: feedback, reflections and support notes where applicable.
- Staff data: employment, training, performance and pre-employment check records.

9. The Digital Academy and online learning

Our Digital Academy (LMS) is a secure platform used to deliver online and blended learning. It records learner registration and engagement, course progress and completion, learner submissions, feedback and activity logs. This data is used to monitor progress and provide personalised support, to meet funder and contractual requirements, to improve course design and delivery, and to generate quality-assurance and performance reports. All Digital Academy data is encrypted in transit and at rest, access-controlled by role, and backed up regularly. Where the platform is operated by a third party, a written data-processing agreement governs their handling of the data.

10. Data sharing and processors

We share personal data only where there is a lawful basis to do so, namely: with authorised personnel within Humanise Solutions on a need-to-know basis; with funders, commissioners or partners where contractually required; and with safeguarding agencies, emergency services or regulators where legally required or to protect an individual from harm. Where we engage processors, we put written agreements in place requiring equivalent security and confidentiality, and we do not permit sub-processing without authorisation. We do not sell personal data, and we do not share it with third parties for their own marketing or commercial use.

11. Data security measures

We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These include:

- Role-based access controls, unique user accounts and strong authentication.
- Encryption of data in transit and at rest, and encrypted or password-protected devices and storage.
- Secure disposal of paper and electronic records at end of retention.
- Regular backups and tested recovery arrangements.
- Confidentiality agreements for all staff who handle personal data.
- Ongoing staff training in data protection and information security.

12. Rights of data subjects

Individuals have the following rights, which we uphold and respond to without undue delay and within one month:

- The right to be informed about how their data is used.
- The right of access to their personal data (a Subject Access Request).
- The right to rectification of inaccurate or incomplete data.
- The right to erasure (the ‘right to be forgotten’), where applicable.
- The right to restrict or object to processing.
- The right to data portability, where applicable.
- Rights related to automated decision-making and profiling (we do not carry out solely automated decision-making with legal or similar effects).

Requests are handled by the Data Protection Officer. We verify the identity of the requester and may, in limited circumstances, extend the response period by up to two months for complex requests, informing the individual within the first month.

13. Personal data breach management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Any suspected breach must be reported immediately to the Data Protection Officer, who will: contain and assess the

breach; record it in the breach log; notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware where the breach is likely to result in a risk to individuals; notify affected individuals without undue delay where the risk is high; and identify and implement actions to prevent recurrence. All breaches and near-misses are reviewed to inform improvement.

14. Records of processing, retention and disposal

We maintain a record of processing activities and a retention schedule that defines how long each category of data is kept. Learner records, management information and quality-assurance evidence are retained only for as long as necessary to deliver our programmes, evidence learner outcomes, satisfy funder and contractual obligations, and support our City & Guilds Assured endorsement and audit trail. At the end of the retention period, data is securely deleted or destroyed. All such documents are controlled, with the latest versions held by Humanise Solutions.

15. Data protection by design and default

We embed data protection into the design of new systems, programmes and processes, collecting the minimum data necessary and applying appropriate safeguards by default. Where a new or changed activity is likely to result in a high risk to individuals, we complete a Data Protection Impact Assessment (DPIA) before processing begins.

16. Training and awareness

All staff, associates and delivery partners receive data protection and information-security training at induction and at regular intervals thereafter, including the safe use of the Digital Academy. Training records are maintained and refreshed in line with our CPD cycle.

17. Roles and responsibilities

- CEO (Policy owner): overall accountability for data protection and compliance.
- Data Protection Officer: advising on compliance, handling rights requests and breaches, ICO liaison and maintaining records of processing.
- Data & Impact Officer (Emily Ward, from 1 March 2026): MI quality, secure and accurate data capture, and reporting accuracy.
- All staff, associates and partners: handling personal data lawfully and securely, and reporting concerns or breaches without delay.

18. Complaints and the ICO

Individuals who are concerned about how we handle their data may raise this with the Data Protection Officer. They also have the right to complain to the Information Commissioner's Office (ico.org.uk). We will cooperate fully with any ICO enquiry.

19. Monitoring, compliance and review

Compliance with this policy is monitored through audits and management review, and forms part of our quality-assurance cycle. This policy is reviewed annually, or sooner where there are significant changes to legislation or to our data-processing activities. For further information, or to exercise your data rights, contact the CEO at scott@humanisesolutions.com · www.humanisesolutions.com.