POLICY

Data Protection Policy

Organisation	Asbiverse Limited trading as Intent Institute (part of Asbiverse Group)
Company number	13891216 (registered in England and Wales)
Registered office	Dairy House, Money Row Green, Holyport, Maidenhead, Berkshire, SL6 2ND
Document reference	II-DP-001
Version	1.0
Issue date	November 2026
Next review	November 2027, or sooner if legislation, guidance or contract requirements change
Approved by	Ankur Shiv Bhandari, Director
Policy owner	Ankur Shiv Bhandari, Director (Data Protection Lead)
Contact	info@intent.institute

> Intent Institute is the Asbiverse Group division for public bodies and other industries, and a trading name of Asbiverse Limited. **This policy applies to all activity of Asbiverse Limited under all its trading names, including Intent Institute and Asbiverse Group, in the United Kingdom and in every other country where we work.**

1. Policy statement

Asbiverse Limited respects the privacy of everyone whose personal data we hold: learners, clients, staff, associates, suppliers and website visitors. We handle personal data lawfully, fairly and securely, and only for clear and legitimate purposes.

2. Scope

This policy applies to all personal data processed by Asbiverse Limited, in any format, and to everyone who handles it for us, including directors, employees, associates, contractors and partners, in the United Kingdom and overseas.

3. Legal framework

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018.
- The Data (Use and Access) Act 2025, which amends both.
- The Privacy and Electronic Communications Regulations 2003 (PECR), for electronic marketing and cookies.

Where we deliver work in the European Union or for EU based clients, we also observe the EU General Data Protection Regulation where it applies.

4. Our role

- **Controller:** Asbiverse Limited is the controller for personal data it decides how and why to use, such as staff, associate, client contact and marketing data.
- **Processor:** When we deliver a contract for a client, such as a public body, we usually process learner and staff data on the client's instructions. We then act as processor under a written contract that meets Article 28 of the UK GDPR.
- **Registration:** Asbiverse Limited will maintain a current registration with the Information Commissioner's Office and pay the data protection fee each year.

- **Data Protection Lead:** Ankur Shiv Bhandari, Director, is responsible for this policy. Asbiverse Limited is not required to appoint a statutory Data Protection Officer, but will do so if its activities change.

5. The data protection principles

We will make sure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes, and not used in ways that are incompatible with them.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Kept no longer than necessary.
- Kept secure.

We are accountable for showing how we comply, and keep records of our processing activities.

6. Lawful basis and sensitive data

- **Lawful basis:** we identify and record a lawful basis before processing personal data. Most of our processing relies on contract, legal obligation or legitimate interests. We use consent only where it is genuinely freely given and can be withdrawn.
- **Special category data:** health information needed for reasonable adjustments, and diversity monitoring data, is collected only where necessary, with an additional condition under the Data Protection Act 2018, and is stored with extra protection.
- **Criminal offence data:** DBS check information is handled only as the law allows for safer recruitment, seen only by those who need it and not kept longer than necessary.
- **Young learners:** learners aged 16 and 17 are children in law. Information given to them is written so they can understand it, and their data receives particular care.

7. Transparency

We tell people what we do with their data through clear privacy notices at the point of collection, including our website privacy notice and the learner privacy notices agreed with each client.

8. Individuals' rights

People have the right to access their personal data, and to ask us to correct, erase or restrict it, to object to its use, to have it transferred and not to be subject to solely automated decisions with significant effects. We will:

- Respond to requests without undue delay and within one month, extended by up to two further months for complex requests as the law allows.
- Carry out a reasonable and proportionate search and verify the identity of the person asking.
- Pass requests about client data to the client promptly where we act as processor, and help the client to respond.

Requests can be made to info@intent.institute or in writing to our registered office.

9. Security

- Access to personal data is limited to those who need it, with strong passwords and multi-factor authentication.
- Devices are encrypted, kept up to date and protected by security software.
- Personal data is shared only through secure, approved systems, never through personal email or messaging accounts.
- Paper records are kept to a minimum, stored securely and shredded when no longer needed.
- We will work towards Cyber Essentials certification and hold it wherever a contract requires it.

10. Suppliers and international transfers

- We use only processors, such as cloud and software providers, that give sufficient guarantees of security, under a written contract.
- Some of our work is supported by colleagues and associates outside the United Kingdom, including our delivery centre in India. Personal data is transferred outside the United Kingdom only where the destination is covered by UK adequacy regulations, or with appropriate safeguards such as the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses, supported by a transfer risk assessment.
- Where we act as processor, we transfer client data overseas only with the client's written authorisation.

11. Data protection by design and impact assessments

We build privacy into new programmes, systems and processes from the start. We carry out a Data Protection Impact Assessment before any processing likely to result in a high risk to individuals, for example new learner tracking or assessment technology, or large scale processing of special category data.

12. Personal data breaches

- Anyone who discovers or suspects a breach must report it to the Data Protection Lead immediately.
- We will contain the breach, assess the risk and record it in our breach log.
- Where required, we will report it to the Information Commissioner's Office within 72 hours of becoming aware of it, and tell the people affected without undue delay if there is a high risk to them.
- Where we act as processor, we will notify the client without undue delay so it can meet its own obligations.

13. Retention

We keep personal data only as long as needed for the purpose it was collected for, then delete or anonymise it securely. Typical periods are set out below. Contract or funder requirements take precedence where they are longer or shorter.

Record	Typical retention period
Learner records for a client contract	As set by the client or funder; otherwise six years after the contract ends
Financial and accounting records	Six years after the end of the financial year
Staff and associate records	Six years after the relationship ends
Unsuccessful job and associate applicants	Six months after the decision
DBS certificate information	Not retained; only the date, type and reference of the check are recorded
Marketing contacts	Until the person opts out, reviewed every two years

14. Marketing

We send electronic marketing only in line with PECR. Every marketing message identifies us and gives a simple way to opt out, and we honour opt outs promptly.

15. Training and complaints

- **Training:** everyone who handles personal data for us receives data protection training when they join and a refresher every year.

- **Complaints:** anyone who is unhappy with how we have handled their personal data can complain to info@intent.institute. We will acknowledge the complaint within 30 days and respond without undue delay. They also have the right to complain to the Information Commissioner's Office at ico.org.uk.

16. Breaches of this policy and review

Breach of this policy by an employee may lead to disciplinary action, and by an associate, contractor or partner to the end of our relationship. The Data Protection Lead reviews this policy every year, or sooner if the law, guidance or our activities change.

Signed	
Name	Ankur Shiv Bhandari
Position	Director, Asbiverse Limited
Date	