



ELEVATE BEYOND LIMITED

GDPR and Data Protection Policy

Supporting Every Step Forward

POLICY INFORMATION	
Date Issued	June 2026
Next Review	June 2027 (annual minimum — or immediately following any change to UK GDPR)
Policy Owner	Sulayman Cham — Founder and Director
Data Controller	Elevate Beyond Limited
ICO Registration Number	ZC149842
ICO Registration Name	Sulayman Cham
Contact for Data Queries	info@elevate-beyond.co.uk 01615248467
Company Number	17222138
Registered Address	Swan Building, 20 Swan Street, Manchester, M4 5JW
ICO Helpline	0303 123 1113 https://ico.org.uk

This policy should be read alongside: Safeguarding and Child Protection Policy, Safer Recruitment Policy, and Candidate Code of Conduct. All four documents form part of Elevate Beyond's compliance framework.

Contents

1. About This Policy
2. Who We Are and What Data We Hold
3. The Data We Collect — Candidates
4. The Data We Collect — Clients and Client Contacts
5. Why We Process Personal Data — Our Legal Bases
6. The Seven Data Protection Principles
7. Special Category and Sensitive Data
8. How We Keep Data Secure
9. Sharing Data with Third Parties
10. How Long We Keep Data — Retention Schedule

-
11. Your Rights Under UK GDPR
 12. Subject Access Requests
 13. The Right to Rectification
 14. The Right to Erasure
 15. The Right to Restrict Processing
 16. The Right to Data Portability
 17. The Right to Object
 18. Consent — How We Obtain and Manage It
 19. Privacy Notices
 20. Data Breaches — Identifying and Reporting
 21. Automated Decision Making
 22. Data Protection Impact Assessments
 23. Responsibilities Within Elevate Beyond
 24. How to Exercise Your Rights or Make a Complaint
-

1. About This Policy

Elevate Beyond Limited takes the privacy of every person whose data we hold seriously. This policy explains how we collect, use, store, share and protect personal data across all of our activities from registering a candidate to invoicing a client setting.

We are required by law to process personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out how we meet those legal obligations and what rights individuals have in relation to the data we hold about them.

This policy applies to everyone whose data Elevate Beyond processes, including registered candidates, client contacts, website enquirers and any third parties with whom we interact in the course of providing our recruitment services.

This policy will be reviewed annually and updated immediately following any significant change to data protection legislation or ICO guidance. Where changes affect how we use your data, we will notify you directly.

2. Who We Are and What Data We Hold

Elevate Beyond Limited is a specialist SEMH and Alternative Provision recruitment agency based in Greater Manchester. We connect tutors, teachers, teaching assistants, learning mentors, HLTAs, LSAs and youth workers with pupil referral units, AP academies, specialist SEND schools and local authority commissioned provisions across all Greater Manchester and other areas.

We are the data controller for the personal data we collect and process. This means we decide why and how personal data is used. We have registered with the Information Commissioner's Office (ICO) as required by law. Our ICO registration number is noted on the cover page of this policy.

As a recruitment agency operating in regulated activity with children, we hold a significant volume of personal data including sensitive data relating to DBS disclosures, right to work documentation and safeguarding records. We take the responsibility of holding this data extremely seriously and apply rigorous security standards to its management.

3. The Data We Collect — Candidates

When a professional registers with Elevate Beyond as a candidate, we collect and process the following categories of personal data:

Identity and Contact Information

- Full name, date of birth and home address.
- Email address and telephone number.
- National Insurance number.
- Photograph where provided.

Professional and Employment Information

- Full employment history including start and end dates, employer names, roles held and reasons for leaving.
- Details of any employment gaps and the reasons provided.
- Professional qualifications and certificates including QTS, QTLS and any SEND-specific qualifications.
- References — the names, roles, and contact details of referees and the content of reference responses.

Compliance and Vetting Data

- Enhanced DBS certificate number, issue date and disclosure level.
- DBS Update Service registration status and date of most recent check.
- Right to work documents such as type, reference number and expiry date.
- Results of online and social media checks.
- Prohibition from teaching check results where applicable.
- Any cautions, convictions or pending matters disclosed during registration.
- Risk assessments conducted in relation to any disclosed information.

Sensitive and Special Category Data

- Criminal record information disclosed through the DBS process.
- Health information provided where relevant to fitness to work.
- Right to work information that may reveal nationality or immigration status.

Placement Records

- Details of placements made such as client settings, dates, role and hours.
 - Timesheet records.
 - Any concerns or incidents arising during a placement.
 - Annual review records and update check dates.
-

4. The Data We Collect — Clients and Client Contacts

When a school, PRU, AP academy or local authority commissions Elevate Beyond's services, we collect and process the following data:

- Organisation name, address and contact details.
- Names, job titles, email addresses and telephone numbers of individuals who act as our contact within the organisation.
- Terms of business and contractual documentation.
- Invoice and payment records.
- Records of placements made to the organisation including candidate names, roles and dates.
- Any safeguarding concerns or incidents reported in connection with a placement.

Client contact data is held for the purpose of managing our commercial relationship with the organisation. We do not use client contact information for marketing purposes without the individual's consent.

5. Why We Process Personal Data — Our Legal Bases

We are required by law to identify a legal basis for processing personal data before we process it. Elevate Beyond relies on the following legal bases depending on the nature of the data and the purpose of the processing:

Contractual Necessity

We process candidate data because it is necessary to fulfil the contract between Elevate Beyond and the candidate. Namely to register them, conduct compliance checks and place them in appropriate settings. We also process client data to fulfil our contractual obligations to supply placement services.

Legal basis: Article 6(1)(b) UK GDPR

Legal Obligation

We are legally required to carry out certain checks under Keeping Children Safe in Education and related legislation. This includes Enhanced DBS checks, right to work verification and the maintenance of a Single Central Record. We process data for these purposes to comply with our legal obligations.

Legal basis: Article 6(1)(c) UK GDPR

Legitimate Interests

We process certain data on the basis of our legitimate interest in running a safe, effective and compliant recruitment business. This includes maintaining records of placements, conducting online checks and retaining records for the purposes of defending any legal claim that may arise.

Legal basis: Article 6(1)(f) UK GDPR

Consent

Where we wish to contact candidates or clients with information about services, updates or opportunities that are not necessary for the performance of our contract, we will ask for your

consent before doing so. You may withdraw this consent at any time by contacting info@elevate-beyond.co.uk.

Legal basis: Article 6(1)(a) UK GDPR — Article 7 conditions apply

Vital Interests and Public Task

In safeguarding contexts, we may be required to share personal data without consent where doing so is necessary to protect a child or vulnerable person from harm. This processing is grounded in our safeguarding obligations and the public interest in protecting vulnerable people.

Legal basis: Article 6(1)(d) and (e) UK GDPR

6. The Seven Data Protection Principles

UK GDPR sets out seven principles that govern how personal data must be handled. Elevate Beyond applies all seven principles to everything it does with personal data:

1. Lawfulness, Fairness and Transparency

We only process personal data where we have a legal basis for doing so. We are open with individuals about what data we hold and why.

2. Purpose Limitation

We collect data for specific, defined purposes and do not use it for anything else without informing the individual.

3. Data Minimisation

We collect only the data we actually need for the purpose in hand. We do not gather data speculatively or hold more than is necessary.

4. Accuracy

We take reasonable steps to keep data accurate and up to date. Where data is found to be inaccurate, we correct or delete it without delay.

5. Storage Limitation

We keep personal data only for as long as it is needed for the purpose for which it was collected. Our retention schedule is set out in Section 10.

6. Integrity and Confidentiality

We protect personal data using appropriate technical and organisational security measures. Data is accessible only to those who genuinely need it.

7. Accountability

We can demonstrate our compliance with all of the above. We maintain records of our processing activities and are prepared to show these to the ICO on request.

7. Special Category and Sensitive Data

Some of the data we process falls into the category of special category data under UK GDPR which is data that is particularly sensitive and that carries a higher level of protection. This includes:

- Criminal record information revealed through DBS checks.

- Health information provided in connection with fitness to work.
- Information that may reveal an individual's racial or ethnic origin through right to work or nationality documentation.

We only process special category data where we have both a lawful basis under Article 6 of UK GDPR and an additional condition under Article 9. In the context of Elevate Beyond's operations, the primary additional conditions are:

- Employment, social security and social protection law which we are required by KCSiE to carry out DBS checks and maintain compliance records.
- Substantial public interest such as safeguarding the welfare of children and young people in SEMH settings.
- Explicit consent where we ask for health information in connection with a candidate's fitness to undertake a particular placement.

Special category data is subject to additional security controls within Elevate Beyond. Access to criminal record information is restricted to the DSL. Health information is held separately from general compliance records and is accessible only to those with a specific need.

8. How We Keep Data Secure

The security of the personal data we hold is a primary responsibility. Elevate Beyond implements the following technical and organisational measures to protect data from unauthorised access, loss, or disclosure:

Access Controls

- Personal data is accessible only to individuals who have a specific and legitimate need to access it in the course of their work for Elevate Beyond.
- Access to sensitive compliance data which includes DBS information and risk assessment records and is restricted to the DSL.
- Passwords must be strong and unique. Multi-factor authentication is used where available.

Device and System Security

- All devices used to process personal data must be password-protected and locked when not in use.
- Elevate Beyond uses up-to-date antivirus and security software on all devices used for business purposes.
- Personal data must not be stored on personal or unencrypted USB drives. Cloud storage used for business data must be password-protected and accessible only via secure login.

Email and Communication Security

- Sensitive personal data must not be transmitted by email without appropriate security measures, such as password protection or secure transfer.
- Candidates and clients will never be asked to send DBS certificates, passport copies or other sensitive documents via unencrypted email.

Physical Security

- Where paper records are held, they must be stored securely and shredded when no longer required.
- Computer screens displaying personal data must not be visible to unauthorised individuals.

Remote and Home Working

- Where work is conducted away from the primary business location, the same security standards apply. Personal data must not be processed on shared or public devices.

9. Sharing Data with Third Parties

Elevate Beyond does not sell personal data to any third party. We share personal data only where it is necessary for the purpose for which it was collected, and only where we have a legal basis for doing so.

The following third parties may receive personal data in connection with our operations:

- Client settings — We share relevant candidate information with client schools, PRUs and local authority provisions when presenting a candidate for a placement. This includes compliance status, qualifications and relevant experience. We do not share DBS certificate information beyond what the client needs to confirm the candidate has passed the required checks.
- uCheck — Our DBS processing provider. Candidate data is shared with uCheck for the purposes of processing Enhanced DBS applications. uCheck is subject to DBS accreditation requirements and processes data in accordance with UK GDPR.
- Danbro (or alternative umbrella company) — Candidate payroll and tax information is shared with the umbrella company for the purposes of administering the candidate's pay. Candidates are informed of this arrangement at the point of registration.
- Xero or FreeAgent — Our accounting software processes client and invoice data for the purposes of financial administration.
- The Disclosure and Barring Service — Where we are legally required to make a referral to the DBS, we will share relevant information as required by law.
- Local Authority Designated Officers (LADOs) and statutory agencies — Where a safeguarding concern or allegation requires referral to statutory agencies, we will share relevant data in accordance with our legal and safeguarding obligations.
- The ICO — We will co-operate with any ICO investigation or audit and will share information as required by law.

Where data is shared with a third party that processes it on our behalf, we ensure that an appropriate data processing agreement is in place. We do not share personal data with any third party in a country outside the UK or the European Economic Area without ensuring that adequate protections are in place.

10. How Long We Keep Data — Retention Schedule

We do not keep personal data for longer than is necessary for the purpose for which it was collected. The following retention periods apply to the main categories of data we hold:

Type of Data	Retention Period	Reason
Candidate compliance records (DBS, references, right to work, SCR entries)	6 years from date registration ends	Legal obligation — employment and safeguarding records
Candidate agreements and code of conduct sign-offs	6 years from date registration ends	Legal obligation — contractual records
Placement records (dates, settings, hours)	6 years from date of placement	Legal obligation — statutory recruitment records
Safeguarding concern records relating to a candidate	6 years minimum — indefinitely where required by statutory guidance	Safeguarding obligation — KCSiE and Working Together
Risk assessment records for DBS disclosures	6 years from date registration ends	Legal obligation — safeguarding and contractual records
Client terms of business and invoices	7 years from date of contract or invoice	Legal obligation — HMRC and Companies Act requirements
Client contact records	3 years from last contact	Legitimate interests — relationship management
Unsuccessful candidate applications	6 months from date of decision	ICO recommended retention for recruitment records
Annual review records	Retained as part of the candidate file for 6 years	Legal obligation — ongoing compliance records
Website enquiry data	12 months from date of enquiry	Legitimate interests — reasonable follow-up period

At the end of the applicable retention period, data will be securely deleted or destroyed. Paper records will be shredded. Digital records will be permanently deleted from all systems and backups.

11. Your Rights Under UK GDPR

Every individual whose data Elevate Beyond holds has the following rights under UK GDPR. These rights apply to both candidates and clients. We will respond to any request within one calendar month of receipt.

Your Right	UK GDPR Article	What This Means for You
Right of Access	Article 15	You can request a copy of the personal data we hold about you at any time.
Right to Rectification	Article 16	If data we hold about you is inaccurate or incomplete, you can ask us to correct it without undue delay.

Your Right	UK GDPR Article	What This Means for You
Right to Erasure	Article 17	You can ask us to delete your data in certain circumstances — for example, where we no longer need it for the purpose we collected it. This right is not absolute and may not apply where we have a legal obligation to retain the data.
Right to Restrict Processing	Article 18	You can ask us to pause processing your data in certain circumstances — for example, while you dispute its accuracy.
Right to Data Portability	Article 20	Where processing is based on your consent or a contract with you and is carried out by automated means, you can ask us to provide your data in a machine-readable format.
Right to Object	Article 21	You can object to us processing your data where we rely on legitimate interests as our legal basis. We will stop processing unless we can demonstrate compelling legitimate grounds that override your interests.
Right to Withdraw Consent	Article 7	Where we rely on your consent to process your data, you can withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing before the withdrawal.

To exercise any of these rights, contact us at info@elevate-beyond.co.uk or call 01615248467. We will respond within one calendar month. In complex cases we may extend this by a further two months, in which case we will tell you within the first month.

12. Subject Access Requests

A subject access request (SAR) is a request by an individual to receive a copy of all the personal data Elevate Beyond holds about them. You have the right to make a SAR at any time, free of charge.

To make a SAR, contact us in writing at info@elevate-beyond.co.uk with the subject line 'Subject Access Request' and include sufficient information for us to identify you and locate your records. We may ask for proof of identity before releasing data.

We will respond to a SAR within one calendar month. Where a request is particularly complex or where multiple requests have been received, we may extend this by a further two months. We will inform you if we need to do this within the first month.

We may decline to comply with a SAR where the request is manifestly unfounded or excessive or where complying would adversely affect the rights and freedoms of other individuals. Where we decline, we will explain our reasons in writing.

13. The Right to Rectification

If you believe that personal data we hold about you is inaccurate or incomplete, you have the right to ask us to correct it. We will action a rectification request without undue delay and in any event within one calendar month.

Where we have shared the inaccurate data with a third party, we will inform that third party of the rectification unless doing so would be impossible or would involve disproportionate effort.

To request rectification, contact us at info@elevate-beyond.co.uk. Please include as much detail as possible about the specific data you believe to be inaccurate and what the correct information should be.

14. The Right to Erasure

You have the right to ask us to delete personal data we hold about you in the following circumstances:

- The data is no longer needed for the purpose for which we collected it.
- You withdraw consent and there is no other legal basis for us to keep the data.
- You object to processing and your interests outweigh our legitimate interests.
- The data has been unlawfully processed.

The right to erasure is not absolute. We may decline an erasure request where we need to keep the data to comply with a legal obligation — for example, our obligation to retain safeguarding and compliance records for a minimum of six years. In these cases, we will explain which data we are required to keep and why.

Where we agree to erase your data, we will delete it from all active systems and ensure it is removed from any backups at the next routine deletion cycle. Where data has been shared with third parties, we will inform them of the erasure request.

15. The Right to Restrict Processing

You can ask us to pause the processing of your personal data without deleting it in the following circumstances:

- You contest the accuracy of the data and want us to pause while we verify it.
- Processing is unlawful but you prefer restriction over erasure.
- We no longer need the data but you need it for a legal claim.
- You have objected to processing and a decision on whether our legitimate interests override yours is pending.

Where processing is restricted, we will continue to store the data but will not use it for any active purpose. We will inform you before lifting any restriction.

16. The Right to Data Portability

Where we process your personal data on the basis of your consent or in connection with a contract and where that processing is carried out by automated means, you have the right to receive a copy of your data in a structured, commonly used and machine-readable format.

You can also ask us to transmit your data directly to another organisation where technically feasible. This right applies to data you have provided to us directly — for example, the information you submitted during the registration process. It does not extend to data we have generated ourselves, such as assessment notes or risk assessments.

17. The Right to Object

Where we process your data on the basis of our legitimate interests, you have the right to object at any time. If you object, we will stop processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms or where we need the data for the establishment, exercise or defence of a legal claim.

You also have an absolute right to object to your data being processed for direct marketing purposes. If you object to marketing, we will stop immediately without needing to consider any competing interests.

18. Consent — How We Obtain and Manage It

Where we rely on your consent as the legal basis for processing your data, we will always obtain that consent in a clear, specific, and informed way. We will never bundle consent requests together with other contractual obligations in a way that makes it unclear what you are agreeing to.

When you give consent, you will be told:

- Exactly what data we want to process.
- Why we want to process it.
- How long we will hold it.
- That you can withdraw your consent at any time.

Consent can be withdrawn at any time by contacting info@elevate-beyond.co.uk. Withdrawal does not affect the lawfulness of any processing that took place before you withdrew consent. However, once consent is withdrawn, we will stop the processing it related to without delay.

We review consent records at least every 24 months to ensure they remain current and relevant. Where circumstances change — for example, if we want to use data for a new purpose we will seek fresh consent rather than relying on the original.

19. Privacy Notices

A privacy notice is a document that tells you how we will use your data at the point we collect it. Elevate Beyond provides privacy notices in the following circumstances:

- At the start of the candidate registration process before any personal data is submitted.
- When a new client contact is added to our records.
- When we collect data for a new or different purpose to the original collection.

Privacy notices are written in plain language. They explain what data we collect, why we collect it, how long we keep it, who we share it with, and what rights the individual has in relation to it.

Where we collect data about an individual from a third party rather than directly from the individual, we will provide a privacy notice to that individual within one month of collecting the data or sooner where we intend to use the data to communicate with them.

20. Data Breaches — Identifying and Reporting

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. This includes incidents such as sending data to the wrong person, losing an unencrypted device or a successful phishing attack.

What to do if you suspect a breach

Anyone associated with Elevate Beyond who suspects that a personal data breach has occurred must report it to the Director immediately. Do not attempt to investigate or resolve the breach independently, report it first.

How Elevate Beyond responds

1. The Director will assess the breach to determine its nature and severity.
2. Steps will be taken immediately to contain the breach and prevent further data loss.
3. Where the breach is likely to result in a risk to the rights and freedoms of any individual, we will notify the ICO within 72 hours of becoming aware of it.
4. Where the breach is likely to result in a high risk to individuals, we will notify those individuals directly and without undue delay.
5. A full record of the breach including the nature of the breach, the data affected, the likely consequences and the steps taken will be documented and retained.

When we must notify the ICO

We must notify the ICO within 72 hours where a breach is likely to result in a risk to people's rights and freedoms. We will report even where we are not certain of the full extent of the breach, and will provide updates as more information becomes available.

ICO: 0303 123 1113 | <https://ico.org.uk/for-organisations/report-a-breach/>

21. Automated Decision Making

Automated decision making means making a decision about an individual using only automated processes without any human involvement. Elevate Beyond does not use automated decision making in any way that produces a legal or similarly significant effect on any individual.

All decisions about candidate registration, placement and vetting are made by Sulayman Cham as the DSL and Director, with full human review of all relevant information. No candidate will be accepted or rejected on the basis of an automated process alone.

We will never use automated decision making or profiling in relation to the personal data of a child.

22. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process for identifying and minimising the data protection risks of a new project or system. Elevate Beyond will carry out a DPIA before introducing any new process, system or technology that is likely to result in a high risk to the rights and freedoms of individuals.

This will include:

- Introducing a new CRM or candidate management system.
- Changing the way we collect, store or share compliance data.
- Using any AI-assisted tool in connection with our recruitment or compliance processes.
- Processing safeguarding data in a new way.

DPIAs will be documented and reviewed before implementation. Where a DPIA identifies a high risk that cannot be mitigated, we will consult the ICO before proceeding.

23. Responsibilities Within Elevate Beyond

Sulayman Cham, as Founder and Director is personally responsible for data protection compliance at Elevate Beyond Limited. This includes:

- Ensuring that this policy is implemented and followed across all of Elevate Beyond's activities.
- Maintaining the ICO registration and keeping it up to date.
- Responding to subject access requests and other rights requests within the required timeframe.
- Overseeing data security and ensuring appropriate technical and organisational measures are in place.
- Reporting data breaches to the ICO where required.
- Reviewing this policy annually and updating it in response to any change in data protection law or ICO guidance.

As Elevate Beyond grows and additional staff are appointed, this policy will be updated to reflect the data protection responsibilities assigned to each role. All staff members, candidates, and contractors who handle personal data on behalf of Elevate Beyond are required to comply with this policy. Failure to do so may result in disciplinary action or termination of engagement.

24. How to Exercise Your Rights or Make a Complaint

If you wish to exercise any of the rights set out in this policy or if you have a concern about how Elevate Beyond has handled your personal data, please contact us using the details below. We will acknowledge your request promptly and respond in full within one calendar month.

Contact for Data Protection Queries

Sulayman Cham — Founder and Director — Elevate Beyond Limited

Email: info@elevate-beyond.co.uk

Phone: 01615248467

Address: Swan Building, 20 Swan Street, Manchester, M4 5JW

Website: www.elevate-beyond.co.uk

If you are not satisfied with our response, or if you believe we have not handled your data in accordance with UK GDPR, you have the right to raise a complaint with the Information Commissioner's Office:

Information Commissioner's Office (ICO)

Telephone: 0303 123 1113

Website: <https://ico.org.uk>

Post: ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Online complaint form: <https://ico.org.uk/global/contact-us/email/>

Elevate Beyond Limited — Supporting Every Step Forward

Company No. 17222138 | info@elevate-beyond.co.uk | www.elevate-beyond.co.uk