SUSSEX TEACHERS LTD

Data Protection Policy

How Sussex Teachers Ltd complies with UK data protection law

Company	Sussex Teachers Ltd ('the Company')
Policy	Data Protection Policy
Applies to	UK GDPR, Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025) and the Privacy and Electronic Communications Regulations 2003 (together, 'the Data Protection Laws')
ICO registration number	A8286918
Policy owner	Michael Bradbury, Director and Data Protection Lead
Version and date	Version 2026.1, effective 1 October 2026. Replaces the policy dated 25 May 2018
Next review	By 1 October 2027, or sooner if the law or our processing changes
Related documents	Privacy Notice; GDPR Policy (including the Appropriate Policy Document, record of processing activities and retention schedule)

1. Introduction and purpose

All organisations that process personal data must comply with data protection legislation. Since 1 January 2021 the law that applies in the UK is the UK GDPR, which sits alongside the Data Protection Act 2018. The Data (Use and Access) Act 2025 amended both, and its main data protection changes came into force on 5 February 2026, with the new requirement for a data protection complaints procedure following on 19 June 2026. This policy replaces our 2018 policy, which referred to the EU General Data Protection Regulation.

As a recruitment business, the Company collects and uses personal data and, because it supplies staff to schools and nurseries, special category data and criminal offence data. This policy sets out how the Company meets its obligations. It should be read with the Privacy Notice and the GDPR Policy.

2. Scope and who must follow this policy

This policy applies to all personal data the Company holds, in any format, about work-seekers, its own staff, individual client contacts, referees and website visitors. It applies to the directors, employees, workers, contractors, consultants and anyone else who handles personal data on the Company's behalf. A breach of this policy by an employee may be treated as a disciplinary matter. Suppliers must meet equivalent standards under their contracts.

3. Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual, such as a name, identification number, location data, online identifier or factors specific to their identity

Term	Meaning
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic or biometric data used to identify someone; data concerning health; and data concerning a person's sex life or sexual orientation. (Previously called 'sensitive personal data'.)
Criminal offence data	Personal data relating to criminal convictions and offences, or related security measures, including cautions, reprimands, warnings and DBS certificate information
Processing	Any operation performed on personal data, including collecting, recording, storing, using, sharing, restricting, erasing or destroying it
Data controller	The organisation that decides the purposes and means of processing. The Company is the controller for the data it holds about work-seekers, staff and client contacts
Data processor	An organisation that processes personal data on behalf of a controller, for example our candidate management system, payroll and cloud storage providers
Consent	A freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or a clear affirmative action, signifying agreement to the processing
Profiling	Any automated processing of personal data used to evaluate personal aspects of an individual, such as work performance, reliability, behaviour or preferences
Pseudonymisation	Processing personal data so that it can no longer be attributed to a person without additional information that is kept separately and protected
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
ICO	The Information Commissioner's Office, the UK supervisory authority for data protection. References to the ICO include any successor body, such as the Information Commission that the Data (Use and Access) Act 2025 provides for

In this policy 'personal data' includes special category data and criminal offence data except where we refer to them specifically.

4. Roles and responsibilities

4.1 **Directors.** The directors are ultimately accountable for compliance and for resourcing it properly.

4.2 **Data Protection Lead (Michael Bradbury).** Oversees day-to-day compliance, maintains the record of processing activities, handles individual rights requests, breaches and complaints, approves new systems and suppliers that involve personal data, and reports to the directors at least annually.

4.3 **Data Protection Officer (Louise Bradbury).** Advises on compliance, monitors it, and is a point of contact for individuals and the ICO. Contact: office@sussexteachers.co.uk.

4.4 **Everyone who handles personal data** must follow this policy, complete data protection training when they start and at least annually, keep personal data secure, and report any suspected breach or request from an individual immediately to the Data Protection Lead.

Details of the people responsible for specific tasks are in the Appendix.

5. How the Company processes personal data

The Company is registered with the ICO (registration number A8286918). It holds personal data for the following purposes:

- staff administration;
- advertising, marketing and public relations;
- accounts and records;
- administration and processing of work-seekers' personal data to provide work-finding services, including processing using software providers and back office support; and
- administration and processing of clients' personal data to supply or introduce work-seekers.

5.1 The data protection principles

The Company will make sure personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes (the Data (Use and Access) Act 2025 sets out when a new purpose is compatible, and we apply it only after recording that assessment);
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date, with inaccurate data erased or corrected without delay;
- kept for no longer than necessary, in line with our retention schedule;
- processed securely, with appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Company is responsible for, and must be able to demonstrate, compliance with these principles (the accountability principle). It does so through the documents and records described in the GDPR Policy.

5.2 Lawful bases for processing

The Company will only process personal data where it has a lawful basis under Article 6 of the UK GDPR, listed in Annex A. For special category data it also needs a condition under Article 9, and for criminal offence data a condition under Article 10 and Schedule 1 of the Data Protection Act 2018 (Annex B). Where the Data Protection Act 2018 requires it, those conditions are supported by the Appropriate Policy Document in the GDPR Policy.

Consent is used only where the individual has a genuine choice. Vetting and safeguarding checks that are legally or contractually required are not based on consent. Where consent is relied on it must be active and informed, recorded with the date, wording and method, and as easy to withdraw as to give. Pre-ticked boxes and silence are not consent.

Where the Company relies on legitimate interests it will complete and record a legitimate interests assessment first. It may rely on the 'recognised legitimate interests' introduced by the Data (Use and Access) Act 2025 only where the specific condition clearly applies.

The Company will review the personal data it holds regularly to ensure it is lawfully processed, accurate, relevant and up to date. Before sharing personal data with any third party, including schools, suppliers, intermediaries and umbrella companies, the Company will establish that it has a lawful reason for doing so.

5.3 Special category and criminal offence data

Schools and nurseries require the Company to process health and criminal offence data to meet statutory safeguarding duties and employment law. The Company relies on the employment condition,

the preventing or detecting unlawful acts condition and the safeguarding of children and individuals at risk condition in Schedule 1 of the Data Protection Act 2018, together with the Appropriate Policy Document. Access to this data is restricted to those who need it, and it is shared only with the school or body that needs it for the specific purpose.

5.4 Privacy by design and by default, and impact assessments

Data protection is built into all processing. This includes data minimisation, pseudonymisation and anonymisation where practicable, role-based access, secure deletion, and cyber security measures. The Company will carry out a data protection impact assessment (DPIA) before any processing likely to result in a high risk to individuals, and before it adopts or migrates to a new candidate management or CRM system, introduces a new AI-assisted tool that handles personal data, or makes any significant change to how special category or criminal offence data is processed.

5.5 Security

The Company protects the confidentiality, integrity, availability and resilience of its systems and services. Measures include access limited to authorised staff on a least-privilege basis, strong authentication, encryption in transit and at rest where the platform supports it, secure storage in approved systems rather than personal devices or personal accounts, backups, patching, clear-desk and screen-lock rules, in-person verification and secure handling of original identity documents, and secure disposal. These measures are tested and reviewed as set out in the GDPR Policy.

5.6 Suppliers and data processors

The Company will use only processors that provide sufficient guarantees of appropriate security. Every processor must be bound by a written contract that meets Article 28 of the UK GDPR, covering processing only on the Company's instructions, confidentiality, security, sub-processors, assistance with individuals' rights and breaches, deletion or return of data, and audit. The Company reviews each key supplier at least annually.

5.7 Transfers outside the UK

The Company holds and processes personal data in the UK and does not routinely transfer it outside the UK. An overseas criminal records check for a work-seeker who has lived abroad is the only expected exception, and only the minimum data needed is sent. Any other transfer requires prior approval from the Data Protection Lead and must be covered by UK adequacy regulations or an appropriate safeguard, such as the ICO's International Data Transfer Agreement or the UK Addendum, supported by a transfer risk assessment confirming that protection is not materially lower than in the UK.

5.8 Children's data

The Company does not collect personal data about children as part of its services. Supply teachers may see pupil information while working in a school. That information belongs to the school, which decides how it is used. Staff placed by the Company must follow the school's data protection and safeguarding policies, must not copy, photograph, remove or store pupil data outside the school's systems, and must report any loss or concern to the school and to the Company at once. The Company does not carry out automated decision-making or profiling using the personal data of children.

5.9 Direct marketing

Marketing is subject to the Privacy and Electronic Communications Regulations 2003 (PECR) as well as the UK GDPR. Since 5 February 2026 PECR breaches can attract fines of up to the same level as UK GDPR fines. Electronic marketing to individuals requires consent or, where PECR allows, a qualifying existing relationship with an easy opt-out. Business to business communications to corporate subscribers are sent only with a clear way to opt out. Every message includes an opt-out, and opt-outs

are actioned promptly and recorded on a suppression list. Individuals can object to direct marketing at any time and the Company must then stop.

6. Rights of individuals

The Company provides information about processing in a concise, transparent, intelligible and easily accessible form, in clear and plain language. It may do so orally if the individual asks.

6.1 Privacy notices

Where the Company collects personal data directly from an individual, it gives them a privacy notice when it first obtains the data. Where it obtains the data from another source, it gives the notice within a reasonable period and at the latest within one month, or when the data is first disclosed to a third party or used to contact the individual, if earlier. If the Company intends to use data for a new purpose it will tell the individual first, unless an exemption applies.

6.2 Subject access requests

Individuals may ask for confirmation that the Company processes their data, a copy of it and the information in the privacy notice. Requests may be made verbally or in writing and in any form. The Company will carry out a reasonable and proportionate search for the data. The response period is one month and starts when the request is received, or later when the Company has received information it reasonably needs to confirm the person's identity or to clarify the request. The Company may extend the period by up to two further months where requests are complex or numerous, and will explain why. Information may be withheld or redacted where an exemption applies, such as the rights of other individuals or legal professional privilege, and the reasons will be given. Third party requests made on behalf of an individual require proof of authority.

6.3 Rectification

Individuals may ask for inaccurate or incomplete personal data to be corrected. The Company will tell any recipients to whom it has disclosed the data about the correction, unless this proves impossible or involves disproportionate effort. The Company cannot audit those recipients to confirm that they have made the correction.

6.4 Erasure

Individuals may ask the Company to erase their personal data in the circumstances set out in Article 17. The Company will refuse to the extent it must keep the data by law or for legal claims, such as vetting, right to work and payroll records, and will explain this. When asked to erase, the Company will ask whether the individual wants all data removed or would prefer the Company to keep a minimal record so that it does not contact them again. Where the Company has made data public it will take reasonable steps to tell other controllers. It will also tell recipients of the data about the erasure unless this proves impossible or involves disproportionate effort.

6.5 Restriction of processing

Individuals may ask the Company to restrict processing where they contest accuracy (while it is checked), where processing is unlawful and they oppose erasure, where the Company no longer needs the data but they need it for legal claims, or where they have objected to processing based on legitimate interests (while the Company decides whether its grounds override theirs). Restricted data is held but not otherwise used, and the Company will tell recipients as in 6.3.

6.6 Data portability

Where processing is based on consent or contract and is carried out by automated means, the individual may receive the data they have provided in a structured, commonly used, machine-readable format and may ask the Company to send it directly to another controller where technically feasible.

6.7 Objection

Individuals may object to processing based on legitimate interests (including profiling). The Company will stop unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights and freedoms, or the processing is needed for legal claims. An objection to direct marketing is absolute and the Company will stop immediately.

6.8 Automated decision-making

The Company does not take decisions about individuals based solely on automated processing where those decisions have a legal or similarly significant effect. The Data (Use and Access) Act 2025 replaced the former Article 22 with new Articles 22A to 22D. Under those rules, decisions based solely on automated processing of special category data remain tightly restricted, and in every other case the Company would have to provide safeguards: information about the decision, the opportunity to make representations, human intervention and the right to contest it. Software, including AI-assisted tools, may support staff, but a person makes and takes responsibility for every decision that affects an individual.

6.9 Handling requests

All requests must be sent immediately to the Data Protection Lead (see the Appendix). Requests are logged and acted on within one month of receipt (adjusted as described in 6.2). The Company may extend the period by up to two further months where necessary, taking into account the complexity and number of requests. There is no fee. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the Company may refuse it or charge a reasonable fee for the administrative cost, and will tell the individual why and about their right to complain.

7. Retention and disposal

Personal data is kept only as long as necessary. The retention schedule in the GDPR Policy sets the periods, which reflect the Conduct of Employment Agencies and Employment Businesses Regulations 2003 (at least one year from creation or from the last time work-finding services were provided), HMRC, national minimum wage and pension requirements, statutory safeguarding guidance and limitation periods. Data is reviewed at the end of each period and then securely deleted or anonymised. Paper records are shredded and electronic records are deleted from live systems and, in due course, backups.

8. Personal data breaches

All suspected breaches must be reported to the persons named in the Appendix immediately, whatever their size. The Company keeps a record of every breach, whether or not it is reported externally.

8.1 **Where the Company is the controller.** The Company will contain and recover the breach, assess the risk, and, where the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO without undue delay and where feasible within 72 hours of becoming aware of it. Where the breach occurs outside the UK, the Company will also alert the relevant supervisory authority in the affected jurisdiction.

8.2 **Where the Company is the processor.** The Company will tell the relevant controller, for example a client school, as soon as it becomes aware of the breach.

8.3 **Telling individuals.** Where a breach is likely to result in a high risk to individuals, the Company will tell the affected individuals without undue delay, in clear language, explaining what happened, the likely consequences, what has been done and what they can do. It need not do so where the data was unintelligible to unauthorised persons (for example because it was encrypted), where subsequent measures mean the high risk is no longer likely to materialise, or where it would involve disproportionate effort, in which case a public communication or similar measure will be used.

9. Human Rights Act 1998

In handling personal data the Company respects the rights of individuals under the Human Rights Act 1998, including respect for private and family life (Article 8), freedom of thought, belief and religion (Article 9), freedom of expression (Article 10), freedom of assembly and association (Article 11) and protection from discrimination in the enjoyment of those rights (Article 14).

10. Complaints

Under the Data (Use and Access) Act 2025, organisations that control personal data must have a procedure for handling data protection complaints, in force from 19 June 2026. The Company's procedure is as follows.

- Individuals can complain by email to the Data Protection Lead or Data Protection Officer, using the complaint form in the GDPR Policy or in their own words. Complaints made verbally or by other routes are accepted and recorded.
- The Company acknowledges every complaint within 30 days, and normally much sooner.
- The Company investigates without undue delay and appropriately, takes steps to respond, keeps the complainant informed, and tells them the outcome without undue delay.
- All complaints and outcomes are logged and reviewed by the directors at least annually to identify improvements.
- Individuals may also complain to the ICO on 0303 123 1113 or at ico.org.uk/make-a-complaint, and may seek a judicial remedy. Complaining to the Company does not affect that right.

11. Training, monitoring and review

Everyone who handles personal data completes data protection training at induction and at least annually, and is given role-specific guidance, for example on handling DBS and health information and on working in schools. Compliance is monitored through the programme of checks set out in the GDPR Policy. This policy is reviewed at least annually and whenever the law, guidance or the Company's processing changes materially, including on migration to a new candidate management system.

Appendix: people responsible

Responsibility	Person
Adding, amending or deleting personal data	Michael Bradbury, Director and Data Protection Lead, and staff authorised by him
Responding to subject access requests and requests for rectification, erasure, restriction, portability, objection and automated decision-making	Michael Bradbury, Data Protection Lead (mike@sussexteachers.co.uk), with the Data Protection Officer

Responsibility	Person
Reporting data breaches and dealing with complaints	Michael Bradbury, Data Protection Lead, and Louise Bradbury, Data Protection Officer
Data Protection Officer	Louise Bradbury (office@sussexteachers.co.uk)

For all of the above, please contact the Director, Michael Bradbury, in the first instance.

Annex A: lawful bases for processing personal data (UK GDPR Article 6)

Basis	When it applies
Consent	The individual has given clear consent for one or more specific purposes
Contract	Processing is necessary for a contract with the individual, or to take steps at their request before entering a contract
Legal obligation	Processing is necessary to comply with the law
Vital interests	Processing is necessary to protect someone's life
Public task	Processing is necessary to perform a task in the public interest or an official function with a basis in law (not normally relied on by the Company)
Legitimate interests	Processing is necessary for the legitimate interests of the Company or a third party, except where those interests are overridden by the individual's interests, rights and freedoms, particularly where the individual is a child. This includes the 'recognised legitimate interests' in Annex 1 of the UK GDPR as inserted by the Data (Use and Access) Act 2025, which the Company uses only where a condition clearly applies

Annex B: conditions for special category and criminal offence data

Processing special category data requires an Article 6 basis and one of the following Article 9 conditions. Many of them also require a condition in Schedule 1 of the Data Protection Act 2018, and some require the Appropriate Policy Document. The conditions the Company most often relies on are marked in the table.

Condition	Use by the Company
Explicit consent (Article 9(2)(a))	Used only for optional health information, where there is a genuine choice
Employment, social security and social protection law (Article 9(2)(b); Schedule 1 paragraph 1)	**Most often used.** Vetting, fitness to work, right to work, reasonable adjustments and statutory pay
Vital interests (Article 9(2)(c))	Emergencies where someone cannot give consent
Manifestly made public by the individual (Article 9(2)(e))	Rarely used
Legal claims (Article 9(2)(f))	Defending or bringing legal claims and responding to complaints

Condition	Use by the Company
Substantial public interest (Article 9(2)(g); Schedule 1 Part 2)	**Often used.** Preventing or detecting unlawful acts (paragraph 10), protecting the public (paragraph 11), safeguarding of children and individuals at risk (paragraph 18)
Occupational medicine and assessing working capacity (Article 9(2)(h); Schedule 1 paragraph 2)	Where a health professional assesses fitness to work in a school
Public health, archiving and research (Article 9(2)(i) and (j))	Not normally relied on
Foundations, associations and not-for-profit bodies (Article 9(2)(d))	Not relevant to the Company

Criminal offence data may be processed only under Article 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018, in the Company's case under paragraphs 1 (employment), 10 (preventing or detecting unlawful acts), 11 (protecting the public) and 18 (safeguarding of children and individuals at risk), supported by the Appropriate Policy Document.