SUSSEX TEACHERS LTD

GDPR Policy

UK GDPR compliance framework and statement of how Sussex Teachers Ltd demonstrates compliance

Company	Sussex Teachers Ltd ('the Company'), an independent, family-owned primary school supply teaching agency, established 2007, based in Brighton and Peacehaven, East Sussex
ICO registration number	A8286918
Policy owner	Michael Bradbury, Director and Data Protection Lead (mike@sussexteachers.co.uk)
Data Protection Officer	Louise Bradbury (office@sussexteachers.co.uk)
Version and date	Version 2026.1, effective 1 October 2026
Next review	By 1 October 2027, or sooner if the law or our processing changes
Law covered	UK General Data Protection Regulation (UK GDPR); Data Protection Act 2018; Data (Use and Access) Act 2025; Privacy and Electronic Communications Regulations 2003 (PECR)
Related documents	Data Protection Policy; Privacy Notice

1. Statement of commitment

Sussex Teachers Ltd is committed to protecting the personal data of the teachers and other staff who work through us, the schools and nurseries we serve, and everyone else whose data we hold. We process personal data only where we need to in order to provide recruitment, safeguarding compliance and payroll services. We aim not only to comply with the UK GDPR but to be able to show, at any time, how we comply.

The Company confirms that it has, and will maintain throughout any contract, the human and technical resources needed to comply with the UK GDPR and to protect the rights of data subjects. This policy describes those resources and measures.

2. Legal framework

Since 1 January 2021 the UK GDPR, which retains the content of the EU GDPR as it applied in the UK, has formed the core of UK data protection law, together with the Data Protection Act 2018. This policy reflects the Data (Use and Access) Act 2025, whose main data protection provisions came into force on 5 February 2026, with the requirement for a data protection complaints procedure following on 19 June 2026. The changes most relevant to the Company are summarised below.

Change	What it means for the Company
Subject access requests: reasonable and proportionate searches; response time runs from receipt of the information needed ('stop the clock')	We search reasonably and proportionately, may pause the one-month clock while we confirm identity or clarify the request, and record when we do (section 8)

Change	What it means for the Company
Data protection complaints procedure (from 19 June 2026)	We provide a way to complain, including an electronic route, acknowledge complaints within 30 days and respond without undue delay (section 11 and Appendix D)
Automated decision-making reform (new Articles 22A to 22D)	We make no solely automated significant decisions about individuals. If that changes we will put in the required safeguards first (section 9)
Recognised legitimate interests and legitimate interests examples	We continue to complete a documented legitimate interests assessment, and use the recognised list only where a condition clearly applies (section 6)
Purpose limitation: new rules on when a different purpose is compatible	We record a compatibility assessment before using data for a new purpose (section 5)
International transfers: 'data protection test' of protection that is not materially lower	We do not routinely transfer data outside the UK, and apply the new test if we ever do (section 12)
Higher PECR fines, now aligned with UK GDPR levels, and new cookie exemptions	We treat marketing compliance as a high-risk area and review cookie use on the website (section 13)
Information Commissioner's Office to become the Information Commission	Our documents refer to the ICO or its successor, and we will update contact details when the change takes effect

3. Governance and accountability

3.1 **Responsibility.** The directors are accountable for compliance. The Data Protection Lead runs the compliance programme day to day. The Data Protection Officer advises on and monitors compliance and is the contact point for individuals and the ICO. Both have direct access to the directors.

3.2 **Resources.** The Company allocates time, training and budget for data protection, uses supplier systems with built-in security controls, and takes specialist advice when needed.

3.3 **Records we keep.** To demonstrate compliance we maintain: a record of processing activities (Appendix A); the Appropriate Policy Document (Appendix B); the retention schedule (Appendix C); a register of data protection impact assessments and legitimate interests assessments; a consent log; a supplier and data processing contract register; a rights request log; a data breach register; a complaints log; and training records.

3.4 **Reporting.** The Data Protection Lead reports to the directors at least annually on requests, breaches, complaints, audit results, supplier reviews and planned improvements.

3.5 **Staff and contractors.** Everyone who handles personal data is bound by confidentiality, is trained at induction and at least annually, and is told that breaches of policy may lead to disciplinary action.

4. What data we hold and why

The Company processes personal data of work-seekers (supply teachers and other education staff), individual client contacts at schools, nurseries and local authorities, its own staff, referees and website visitors. This includes special category data (health information) and criminal offence data (DBS information) that schools and the law require us to check. Appendix A records each activity, its purpose, lawful basis, recipients, retention period, transfers and security.

Data is processed only for recruitment, safeguarding compliance and payroll purposes, and for the running of the business, including marketing to schools. We do not use it for unrelated purposes and we do not sell it.

5. The data protection principles in practice

Principle	How we comply
Lawfulness, fairness and transparency	Every activity has a documented lawful basis (Appendix A). Individuals receive our Privacy Notice at registration, or within one month where we obtain data from another source
Purpose limitation	Purposes are recorded in advance. Before using data for a new purpose we record whether it is compatible with the original purpose under the UK GDPR as amended by the Data (Use and Access) Act 2025, and tell individuals where required
Data minimisation	We collect only what vetting law, safeguarding guidance, payroll and client contracts require. Forms are reviewed annually to remove unnecessary fields
Accuracy	Candidates confirm their details on registration and at least annually. Corrections are made promptly and passed to recipients. School contact details are checked against public sources
Storage limitation	The retention schedule (Appendix C) sets a period for every category. Records are reviewed at least every six months and deleted securely when the period ends
Integrity and confidentiality	Security measures in section 7, tested as set out in section 14
Accountability	The records in section 3.3, regular audits and reporting to the directors

6. Lawful basis, consent and legitimate interests

6.1 **Choosing a basis.** Before processing begins, the Data Protection Lead confirms the lawful basis under Article 6 and, for special category and criminal offence data, the Article 9 or 10 condition and Schedule 1 condition (Appendix B). The basis is recorded in Appendix A.

6.2 **Vetting is not based on consent.** Identity, right to work, DBS, barred list, TRA, fitness to work and similar checks are carried out because the law, statutory safeguarding guidance and our contracts with schools require them. We rely on legal obligation, contract, legitimate interests and the employment and safeguarding conditions, not consent. Our 2018 materials that described consent as the basis for health and criminal records data have been replaced.

6.3 **Where consent is used.** This covers optional matters such as electronic marketing to individuals where PECR requires consent, and optional health information a work-seeker chooses to add. Consent must be a clear affirmative act, specific to the purpose, freely given and informed. We never use pre-ticked boxes or bundle consent into terms.

6.4 **Consent records are auditable.** For each consent we record who consented, the date and time, what they were told (the version of the notice or wording), how they consented, and any withdrawal. Withdrawal is as easy as giving consent and takes effect promptly. Consent is refreshed if purposes change.

6.5 **Legitimate interests.** We complete a three-part assessment (purpose, necessity, balancing) before relying on legitimate interests, keep it on file and review it annually. The recognised legitimate interests introduced in 2026 are used only where the specific condition clearly applies.

7. Security: confidentiality, integrity, availability and resilience

The Company applies technical and organisational measures proportionate to the risk, including to the special category and criminal offence data it holds.

Area	Measures
Confidentiality	Candidate and school data held only in the Company's CRM and candidate management system and secure OneDrive cloud storage. Access is limited to authorised staff on a least-privilege basis, with named user accounts and strong, unique authentication. Confidentiality duties apply to everyone with access. Original identity and qualification documents are checked in person at registration. Health and DBS information is restricted to those who need it. No personal data is stored on personal accounts or removable media
Integrity	Changes are made through controlled systems with an audit trail where the platform provides one. Data entry and compliance checks are reviewed. Inaccurate data is corrected promptly. Devices and software are kept up to date with security patches, and anti-malware protection is in place
Availability and resilience	Cloud-hosted systems with provider-managed redundancy and backup. Data can be restored after loss or corruption, and restoration is tested at least annually. A business continuity approach covers loss of devices, accounts or suppliers, including a documented way to contact work-seekers and schools without the main system
Devices and access	Screen locks, encryption of laptops and phones where supported, immediate reporting and remote wipe for lost devices, and prompt removal of access when someone leaves or changes role
Physical	Paper records are kept to a minimum, held in locked storage and shredded when no longer needed. Original documents are returned to the individual after checking
Disposal	Secure deletion from live systems at the end of the retention period, and shredding of paper
Suppliers	Security assessed before onboarding, written contracts that meet Article 28, and annual review (section 10)

The Company plans to migrate to a new, more tightly access-controlled candidate management system in 2026/27. A data protection impact assessment, supplier security review, data mapping and a tested migration and deletion plan will be completed before any live data is moved, and this policy and the Privacy Notice will be updated as needed.

8. Rights of individuals and how we handle requests

The Company respects the rights to be informed, of access, to rectification, to erasure, to restriction, to data portability, to object, to withdraw consent, and in relation to automated decision-making. Requests may be made in any form, verbally or in writing, to any member of staff, and must be passed to the Data Protection Lead the same day.

Step	What we do	Time
1. Log	Record the request, date received, requester and what is asked for in the rights request log	Same working day
2. Acknowledge and verify	Confirm receipt. If identity is uncertain, or the request is unclear, ask for the minimum information needed. The one-month period runs from receipt, or from receipt of that information if later, and we record the date	Within 3 working days
3. Search	Carry out a reasonable and proportionate search of the CRM, email, OneDrive and other systems and processors that hold the data	Within the first 2 weeks
4. Assess	Decide what must be provided, corrected, erased, restricted or ported, and what exemptions apply (for example, the rights of other people, legal professional privilege or legal retention duties)	Before week 4
5. Respond	Provide the response in a clear, commonly used format with the required supplementary information. Where we refuse or restrict, explain why and give the right to complain to us and to the ICO	Within one month of the start date
6. Extend (if needed)	For complex or numerous requests, extend by up to two further months and tell the individual within the first month and why	By the end of month one
7. Notify recipients	Tell recipients of any rectification, erasure or restriction, unless impossible or disproportionate	On completion
8. Close	Record the outcome, time taken and any learning	On completion

Requests are free of charge. We may refuse, or charge a reasonable fee for, a request that is manifestly unfounded or excessive, and will say why. Vetting, right to work and payroll records cannot normally be erased during their legal retention period, and we will explain this to the individual. Objections to direct marketing are always actioned.

9. Automated decision-making, profiling and AI-assisted tools

The Company does not make solely automated decisions with a legal or similarly significant effect on individuals, and does not use the personal data of children for automated decision-making or profiling. Any new software, including AI-assisted tools, that will handle personal data requires a data protection impact assessment, a review of the supplier's terms (including whether data is used to train models and where it is stored), and approval by the Data Protection Lead before use. A person must review any output before it is used in a decision about an individual. If the Company ever introduced a solely automated decision, it would first provide the safeguards required by Articles 22A to 22D: information about the decision, an opportunity to make representations, human intervention and the right to contest it. For special category data the rules are stricter, and such a decision would not be taken without a clear legal basis.

10. Suppliers and data processors

- Due diligence before engagement: security standards, certifications where relevant, location of processing, sub-processors, breach history and ability to support individuals' rights.

- A written contract that meets Article 28 of the UK GDPR, with processing only on our documented instructions, confidentiality, security, sub-processor controls, assistance with rights requests, prompt breach notification, return or deletion of data at the end, and audit rights.
- An entry in the supplier register recording what data each supplier holds, where, and the contract date.
- An annual review of each key supplier, and a review whenever the service or its terms change materially.
- Sharing with controllers such as client schools, vetting bodies and HMRC on the basis of a lawful reason recorded in Appendix A.

11. Personal data breaches and complaints

11.1 Breach response

Anyone who suspects a breach must report it to the Data Protection Lead immediately. The response is as follows.

Stage	Action	Time
Contain	Stop the breach, recover data where possible, revoke access, change credentials	Immediately
Assess	Establish what data, how many people, what harm is likely (including whether special category or criminal offence data is involved), and whether the data was protected, for example by encryption	Within 24 hours
Record	Enter the breach, its effects and our actions in the breach register, whether or not it is reportable	Within 24 hours
Notify the ICO	If the breach is likely to result in a risk to individuals, report to the ICO online or on 0303 123 1113	Without undue delay and where feasible within 72 hours of becoming aware
Notify controllers	If we are acting as a processor, tell the controller (for example a client school) without undue delay. If a school-held record is involved, liaise with the school	Without undue delay
Notify individuals	If the breach is likely to result in a high risk, tell affected individuals clearly and without undue delay, with advice on how to protect themselves	Without undue delay
Review	Find the cause, fix it and update procedures and training	Within 30 days

11.2 Complaints procedure

The Company has a data protection complaints procedure in line with the Data (Use and Access) Act 2025.

- Individuals can complain by email to the Data Protection Lead (mike@sussexteachers.co.uk) or Data Protection Officer (office@sussexteachers.co.uk), using the complaint form at Appendix D, which can be completed and returned electronically, or in their own words.
- We acknowledge every complaint within 30 days of receipt, and we aim to do so within five working days.
- We investigate to the extent appropriate, keep the complainant informed, and tell them the outcome without undue delay.

- We log each complaint and outcome and review the log annually to improve.
- Individuals can also complain to the ICO (ico.org.uk/make-a-complaint, 0303 123 1113) and seek a remedy in court.

12. International transfers

The Company stores and processes personal data in the UK and does not routinely transfer personal data 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 to the relevant authority. No other transfer may take place without prior written approval from the Data Protection Lead. Any approved transfer must be covered by UK adequacy regulations or an appropriate safeguard, such as the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment showing that the protection given to the data is not materially lower than in the UK. Before engaging any supplier we confirm where their servers and support staff are located. Any transfer is recorded in Appendix A and in the Privacy Notice.

13. Marketing and cookies

Electronic marketing complies with PECR and the UK GDPR. Individuals are marketed to only with consent or, where PECR allows, on the basis of an existing relationship with a clear opt-out. Business to business emails to corporate subscribers carry an opt-out. Suppression lists are kept and honoured. Website cookies that are not strictly necessary or covered by an exemption are set only with consent, the cookie banner is reviewed at least annually, and where we rely on the exemption for statistical cookies we give clear information and a simple way to object.

14. Monitoring, testing and review

The Company regularly tests, assesses and evaluates the effectiveness of its measures. The programme below is recorded and reported to the directors.

Check	Frequency
Review of user accounts and access rights, and removal of leavers	Quarterly
Review of records for accuracy, retention and secure deletion	Six-monthly
Backup restoration test	Annually
Breach response and rights request exercise (a desk-top test)	Annually
Internal audit against this policy, including a sample of candidate files for lawful basis, privacy notice delivery and consent records	Annually
Supplier review and contract check	Annually
Review of the record of processing, DPIAs, legitimate interests assessments and cookie use	Annually, and on any significant change
Staff training and refresher	At induction and annually
Review of this policy, the Data Protection Policy and the Privacy Notice	Annually, and when the law or processing changes

Appendix A: Record of processing activities

This record is kept under Article 30 of the UK GDPR. The Company holds special category and criminal offence data as a regular part of its work, so the record applies in full.

Activity and purpose	People and data	Lawful basis and conditions	Recipients and transfers	Retention
Work-seeker registration and matching to assignments	Supply teachers and other education staff. Identity, contact details, CV, qualifications, availability	Contract; legitimate interests	Client schools and nurseries. CRM and cloud providers. No transfers outside the UK	See Appendix C
Vetting and safeguarding compliance	Work-seekers. ID, right to work, DBS, barred list, TRA, references, fitness to work (special category), criminal offence data	Legal obligation; legitimate interests. Article 9(2)(b), Schedule 1 paras 1, 10, 11 and 18; Article 10	Schools, GBG Group Plc, DBS, TRA, UKVI and Home Office, referees. Overseas criminal records agencies only where required	See Appendix C
Payroll, tax and pensions	Workers. Bank, tax, NI, pension and pay data	Contract; legal obligation	Payroll and accountancy providers, HMRC, pension provider	Six years from the end of the tax year
Assignment management, feedback and concerns	Workers. Assignments, feedback, concerns and allegations	Legitimate interests; legal obligation. Article 9(2)(b) and (f), Schedule 1 para 18 where relevant	Schools, DBS, TRA, local authority designated officer, where required	See Appendix C
School and client contact management and marketing	Contacts at schools, nurseries and local authorities. Name, role, work contact details, interactions	Legitimate interests; PECR corporate subscriber rules	CRM and email providers. No transfers outside the UK	Reviewed at least every two years
Marketing and job alerts to individuals	Work-seekers and prospects. Contact details, preferences	Consent or PECR existing relationship; legitimate interests	Email marketing provider. No transfers outside the UK	Until opt-out, then a minimal suppression record
Staff administration	The Company's own staff. Contract, payroll, absence	Contract; legal obligation. Article 9(2)(b)	Payroll provider, HMRC, pension provider	Six years after employment ends
Accounts and records	Clients and suppliers. Business and invoice data	Contract; legal obligation	Accountants, HMRC	Six years
Website and enquiries	Visitors and enquirers. IP address, cookie data, messages	Legitimate interests; consent for non-essential cookies	Website host and analytics provider	As stated in cookie notice; enquiries up to 12 months

Activity and purpose	People and data	Lawful basis and conditions	Recipients and transfers	Retention
Complaints, disputes and legal claims	Complainants and others. Details of the matter	Legitimate interests; legal obligation. Article 9(2)(f)	Advisers, insurers, regulators	Six years from closure

Appendix B: Appropriate Policy Document

This is the appropriate policy document required by Schedule 1 Part 4 of the Data Protection Act 2018 where the Company processes special category data and criminal offence data under the employment condition (paragraph 1) and the substantial public interest conditions (including paragraphs 10, 11 and 18). It is reviewed annually and kept until six months after processing under these conditions stops. It is made available to the ICO on request.

B.1 Conditions relied on

- **Employment, social security and social protection law (Schedule 1 paragraph 1):** pre-engagement vetting and fitness-to-work checks, right to work, reasonable adjustments and statutory pay.
- **Preventing or detecting unlawful acts (paragraph 10), protecting the public against dishonesty and unfitness (paragraph 11) and safeguarding of children and individuals at risk (paragraph 18):** DBS and barred list checks, safeguarding information and the sharing of it with schools, the DBS and the TRA.
- **Occupational medicine (paragraph 2) and legal claims (Article 9(2)(f)):** fitness-to-work assessments and the defence of claims.

B.2 How we comply with the principles

Principle	Our procedures
Lawfulness, fairness and transparency	We process this data only where a Schedule 1 condition applies, and tell individuals in the Privacy Notice what we collect and why
Purpose limitation	It is used only for vetting, safeguarding, fitness-to-work and related legal purposes and is not reused for marketing or unrelated purposes
Data minimisation	We hold only the outcome and details we need, for example the DBS certificate number, date and result. We keep copies of certificates for no longer than six months
Accuracy	Checks are repeated or updated (for example using the DBS Update Service with the individual's consent) and inaccurate records are corrected promptly
Storage limitation	Retention periods are set in Appendix C. Records are reviewed and securely deleted when the period ends
Security	Access is limited to named staff who need it. Records are held in secured systems. Disclosures to schools are made only to the relevant recipient and are logged
Accountability	Recorded in Appendix A. Reviewed annually by the Data Protection Lead, who reports to the directors

B.3 Retention and erasure

Special category and criminal offence data is kept in line with Appendix C. When the retention period ends it is securely deleted. Individuals can ask us to erase their data and we will do so unless we must keep it by law or for legal claims, in which case we explain this to them.

Appendix C: Retention schedule

Data	Retention period	Reason
Work-seeker registration records	At least one year from creation or from the date work-finding services were last provided, whichever is later. Then reviewed and deleted unless there is a reason to keep	Conduct of Employment Agencies and Employment Businesses Regulations 2003
Unsuccessful or incomplete registrations	Up to 12 months, then deleted	Business need; storage limitation
Right to work evidence	Duration of the work relationship plus two years	Immigration, Asylum and Nationality Act 2006 and Home Office guidance
DBS information	Record of date, number and outcome kept with the vetting record. Copy of the certificate kept for no longer than six months	DBS code of practice and safeguarding guidance
Vetting records, references and compliance checklists	Duration of the work relationship plus six years	Evidence for schools and inspectors; legal claims
Payroll, tax, holiday pay, sick pay, pension auto-enrolment, timesheets	Six years from the end of the relevant tax year	HMRC, national minimum wage, social security, pension and working time legislation; limitation period
Safeguarding concerns, allegations and outcomes	Until normal retirement age or 10 years from the allegation, whichever is longer. Removed if found false or malicious	Statutory safeguarding guidance
Complaints and legal claims	Six years from closure	Limitation period
Marketing preferences	Until opt-out, then a minimal suppression record	PECR and UK GDPR
School and client contact data	While relevant, reviewed at least every two years	Legitimate interests; accuracy
Breach, rights request and complaints registers	Six years	Accountability and limitation period
Staff records	Six years after employment ends	Employment and tax law

Appendix D: Data protection complaint form

You can complete this form and email it to mike@sussexteachers.co.uk or office@sussexteachers.co.uk. You do not have to use this form. You can also complain in your own words, by email, by telephone or in writing. We will acknowledge your complaint within 30 days and tell you the outcome without undue delay.

Question	Your answer
Your full name	
Your contact email and telephone number	
Your relationship to us (for example, work-seeker, school contact, other)	
What happened? Please describe what you are unhappy about, including dates if you can	
What data is involved, if you know?	
What would you like us to do to put things right?	
Have you already contacted us about this? If so, when and with whom?	
Date	

If you are not satisfied with our response, you can complain to the Information Commissioner's Office at ico.org.uk/make-a-complaint or on 0303 123 1113.