Bespoke

Tutors UK Ltd.

67 King Street, Maldon, Essex. CM9 5DX

Company registration no.: 14831085

Data Protection Policy

Last Updated: 30.08.23

Reviewed on: 30.08.24

Statement of intent

This policy aims to ensure that all personal data collected about tutors, students and their families is collected, stored and processed in accordance with the General Data Protection Regulation (EU) (GDPR, 2018) and the Data Protection Act 2018 (DPA 2018).

Bespoke Tutors UK Ltd. is required to keep and process certain information about its staff members, contractors (including tutors), consultants, partners, tutees and other third parties in accordance with its legal obligations under the EU General Data Protection Regulation (GDPR 2018).

We may, from time to time, be required to share personal information about its staff or pupils with regulatory services, and potentially, children's services.

This policy is in place to ensure all staff and clients are aware of their responsibilities and outlines how Bespoke Tutors UK Ltd, complies with the core principles of the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

1. GDPR Definitions:

Personal data:

Any information relating to an identified, or identifiable, living individual. This may include the individuals:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data:

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing:

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject

The identified or identifiable individual whose personal data is held or processed.

Data Controller

A person or organisation that determines the purposes and the means of

processing of personal data.

Data Processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

2. Data Control

Bespoke Tutors UK Ltd. processes personal data relating to tutors, students and their families and are therefore, data controllers.

3. Roles and Responsibilities

This policy applies to all individuals engaged by Bespoke Tutors UK Ltd. to provide services.

3.1 Data Protection

Bespoke Tutors UK Ltd. is responsible for overseeing the implementation of this policy and monitoring compliance with data protection law.

3.2 All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Following up:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

4. Legal framework

4.1. This policy has due regard to legislation, including, but not limited to the following:

The General Data Protection Regulation (GDPR), The Freedom of Information Act 2000, The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016), The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

4.2. This policy will be implemented in conjunction with the following policies/documents:

- Safeguarding Policy
- Privacy Notices
- Online Safety Policy
- Terms of Business

5. Data Protection Principles

The GDPR is based on data protection principles that Bespoke Tutors UK Ltd. must comply with.

5.1 The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

5.2. The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”. (“Accountability”)

This policy sets out how Bespoke Tutors UK Ltd. aims to comply with these principles.

6. Sources

For the purposes of business, personal or sensitive information may derive from various sources, such as:

- Employees (and close relations, e.g. emergency and next of kin contacts).
- Ex-employees.
- Potential and prospective employees.
- Referees.
- Client records.
- Targeted school individuals (marketing).
- School pupils.
- Tutors.

7. Accountability

7.1. Bespoke Tutors UK Ltd. will demonstrate accountability by implementing policies and procedures, technical and organisational measures and keeping documentation such as breach records and DSAR records.

7.2. We will provide comprehensive, clear and transparent privacy policies.

7.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

7.4. We will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Anonymising
- Transparency.

- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

7.5. Data protection impact assessments (DPIA) are used, where appropriate.

8. Data protection officer (DPO)

8.1. The DPO has been appointed in order to:

- Inform and advise employees and contractors about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments and providing the required training to staff members.

8.2. The DPO will be responsible for overseeing the company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

8.3. The DPO will operate independently in performing their DPO duties.

8.4. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

9. Lawful processing

9.1. The legal basis for processing data will be identified and documented prior to data being processed.

9.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for: Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, for the performance of a contract with the data subject or to take steps to enter into a contract, protecting the vital interests of a data subject or another person, for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by us in the performance of its tasks.)

9.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject

10. Consent

10.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. For the purposes of our services, consent must be a written agreement.

10.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

10.3. Where consent is given, a record will be kept documenting how and when consent was given.

10.4. We ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

10.5. Consent can be withdrawn by the individual at any time.

10.6. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents (through the school) will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

11. Collecting personal data

11.1. Lawfulness, fairness and transparency

We will only process personal data where we have 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that we can fulfil a contract with the individual, or the individual has asked the office to take specific steps before entering into a contract.
- The data needs to be processed so that we can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed for legitimate interests (where the processing is not for any tasks the school performs as a public authority) or a

third party, provided the individual's rights and freedoms are not overridden

- The individual (or their parent/carer when appropriate in the case of a student has freely given clear consent) For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:
    - The individual (or their parent/carer when appropriate in the case of a student) has given explicit consent
    - The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
    - The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
    - The data has already been made manifestly public by the individual
    - The data needs to be processed for the establishment, exercise or defence of legal claims
    - The data needs to be processed for reasons of substantial public interest as defined in legislation
    - The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
    - The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
    - The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

11.2. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

12. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so.

These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff. Where we transfer personal data internationally, we will do so in accordance with data protection law.

13. Subject access requests and other rights of individuals

13.1. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that we hold about them.

This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the Data Protection Officer

13.2. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

13.3. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the

request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

13.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Data Protection Officer. If staff receive such a request, they must immediately forward it to the Data Protection Officer.

14. Parental requests to see the educational record

Parents, or those with parental responsibility, can request in writing access to their child's educational record.

We shall provide this within 15 school days of receipt of the request. This right applies as long as the pupil concerned is aged under 18. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual.

Regular reviews with parents and the child will be held, usually every 6 weeks and written progress reviews are available upon written request.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office or left anywhere else where there is general access
- Passwords containing letters and numbers are used to access electronic devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

We will act lawfully when keeping or disposing of any personal data held on fil

17. Personal data breaches

Bespoke Tutors UK Ltd. will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data about students and their families.

18. Legitimate Interests

Bespoke Tutors UK Ltd. relies on the legitimate interest basis for some of their uses of constituents' personal data, like performing analytics. Using legitimate interest requires that we:

- Conduct a balancing test.
- Tell constituents that you're relying on legitimate interests;
- Allow constituents to opt out of the processing.

19. Training

All staff should undergo data protection training. All contractors will be offered the opportunity to access regular training however, this is optional.

20. DBS data

20.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

20.2. Data provided by the DBS will never be duplicated.

20.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

21. Videos and photography

21.1. We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. We will always indicate its intentions for taking photographs of pupils and tutors and will retrieve permission before publishing them.

21.3. If we wish to use images/video footage of pupils in a publication, written permission will be sought for the particular usage from the parent of the pupil.

22. Employee Responsibilities

22.1. Compliance with this Policy is the responsibility of every employee (including temporary employees and consultants), and any person who acts on behalf of Bespoke Tutors UK Ltd. and any person who has responsibilities for the collection, access or processing of personal data.

22.2. Employees must understand what is meant by personal and sensitive data, and know how to handle such data.

22.3. Each employee of The Tutor Trust is required to:-

- Read and understand this Data Protection Policy.
- Complete and pass compulsory GDPR online training and read updates as directed.

- Adhere and abide to this Data Protection Policy.
- Share best practices on data protection issues.
- Read and adhere to any changes or updates to this Data Protection Policy when notified of such changes or updates.
- Report concerns relating to data protection to the DPO.

23. Contractor Responsibilities

23.1. All contractors, Data Processors, agents, consultants, partners, sub-contractors and other third parties acting on behalf of Bespoke Tutors UK Ltd., including tutors, must:

- Ensure that they and all employees who have access to personal data held or processed for on our behalf, are aware of this policy and are fully aware of their duties and responsibilities under the GDPR
- Any breach of any provision of GDPR will be deemed as being a breach of any contract between us and that individual, company, partner, organisation or firm
- Allow data protection audits by Bespoke Tutors UK Ltd. of personal data held on its behalf (if requested)
- Indemnify us against any prosecution, claims proceedings, actions or payments of compensation or damages, without limitation.

23.2. All contractors, Data Processors, agents, consultants, partners, sub-contractors and other third parties who are users of personal data supplied by Bespoke Tutors UK Ltd. must confirm they have a compliant data protection register entry in the ICO's public register, and must provide security guarantees at least equivalent to the technical and organisational measures we have adopted to ensure compliance with the GDPR Act.

24. Policy review

24.1. This policy is reviewed annually by the DPO and approved by the Company Director.

22.2. The next scheduled review date for this policy is August 2024.

For further information please contact:

Data Protection Officer

Bespoke Tutors UK Ltd.

67 King St., Maldon. Essex. CM9 5DX.

T: 07488 386703 | E: Bespoketutorsuk@gmail.com

Signed by: ***K Marshall***

Position: Company Director

Date*: 30.08.23*

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer.

They will investigate the report, and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been.
- Made available to unauthorised people

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary

They will assess the potential consequences, based on how serious they are, and how likely they are to happen

They will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, they must notify the ICO. They will document the decision (either way), in case it is challenged

at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:

  - The categories and approximate number of individuals concerned

  - The categories and approximate number of personal data records concerned

  - The name and contact details of the DPO

  - A description of the likely consequences of the personal data breach

  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. They will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the office will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the reporting officer
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above, any decision on whether to contact individuals will be documented by the DPO and Company Director

- We will notify any relevant third parties who can help mitigate the loss to

individuals – for example, the police, insurers, banks or credit card companies

- They will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

  - Facts relating to the breach

  - Effects

  -n Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored. A review will be carried out so that it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender as they become aware of the error

In any cases where the recall is unsuccessful, we will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

We will ensure they receive a written response from all the individuals who received the data, confirming that they have complied with this request. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.