



Privacy Policy

Introduction

The official business name of the company is Brilliant Coaching and Development, and this name will be used throughout the policy.

1. Aims

Brilliant Coaching and Development is committed to taking data protection very seriously. This policy sets out the measures the business will implement to ensure the protection of all personal and sensitive data relating to pupils, clients, and all other individuals.

2. Legislation and Guidance

The General Data Protection Regulation (GDPR) came into force in May 2018 as part of the Data Protection Act 2018 (DPA 2018), which replaced the previous Data Protection Act 1998. GDPR concerns the collection, processing, and storage of personal data. This policy is based on guidance published by the Information Commissioner's Office (ICO), including the ICO's code of practice for subject access requests.

3. Definitions

This policy uses the following terminology with the corresponding definitions:

Terminology	Definition
Processing	Any action or operation performed on personal data, such as collecting, recording, storing, altering, using, transmitting, destroying, or erasing. Processing also includes transferring personal data to third parties.
Data Subject	Any person about whom we hold personal data. In the context of the school, this could include pupils, parents, staff, governors, volunteers, and visitors.
Personal Data	Any information that relates to an identified or identifiable (either directly or indirectly) person or data subject.
Sensitive Data	Information relating to special categories that require extra security. These categories include: racial or ethnic origin data, political opinions, religious or philosophical beliefs, trade union membership, genetic data, and biometric data.
Data Controller	The individual, agency, or authority who decides how and why data is processed. In this policy, the school is the data controller.

Data Processor	The individual, agency, or authority that processes data on behalf of a data controller.
Data Protection Officer (DPO)	The person responsible for independent and impartial monitoring and application of laws that protect personal data within the school.
Data Breach	A breach of security that leads to the accidental or unlawful loss, destruction, alteration, disclosure, or access to personal data while stored, transmitted, or being processed. Such incidents must be reported to the Information Commissioner's Office (ICO).
Information Commissioner's Office (ICO)	A UK-based organisation responsible for upholding information rights.
Data Users	Individuals who process personal data. They must protect data in accordance with this data protection policy.
Data	Information stored electronically, on a computer, or in certain paper-based filing systems.

4. Data Protection Principles

To comply with GDPR, Brilliant Coaching and Development must adhere to the following data protection principles:

- Personal data must be processed lawfully, fairly, and in a transparent manner.
- Personal data must be collected for legitimate purposes.
- Personal data must be relevant and limited to what is necessary to fulfil the purposes for which it is stored, and retained for no longer than is necessary.
- Personal data must be processed in a way that ensures it is appropriately secure.

This policy explains how the company ensures compliance with these principles.

5. Collecting Personal Data

Collecting personal data is an essential part of the daily operations of Brilliant Coaching and Development. Personal data will only be collected for specific, explicit, and legitimate reasons. These reasons will be explained to individuals at the point of data collection.

6. Sharing Personal Data

Sharing personal data is sometimes necessary for the effective operation of Brilliant Coaching and Development. To ensure lawful sharing of personal data, the following procedures are observed:

Scenario	Procedure
Regulatory Bodies (e.g. government agencies or healthcare)	Before sharing personal data with a regulatory body requesting access, the DPO will verify the identity of the body and investigate how the data will be used. Only when satisfied will Brilliant Coaching and Development share any personal data.
Suppliers or Subcontractors Requiring Access to Personal Data	The DPO will assess all suppliers and subcontractors for GDPR compliance. They must read and follow the school GDPR policy before being granted access to personal data.
The Police	The police may only request access to data with a relevant warrant.

7. Data Retention, Security and Storage

Brilliant Coaching and Development will only store data that is adequate, purposeful, necessary, and limited to what is essential. Stored data will be protected from unauthorised access and data breaches through current and well-maintained security protocols, ensuring confidentiality, integrity, and availability:

- Confidentiality: Only authorised individuals can access data.
- Integrity: Data is accurate and suitable; inaccurate or unsuitable data will not be retained.
- Availability: Those authorised to access the personal data can do so when required.

Data Type	Security Measures
Paper Records	All paper records stored on site will be kept in a secure and locked location. Only authorised individuals will be granted access.
Portable Electronic Devices (e.g. Laptops, iPads)	All portable electronic devices will be password protected. Laptop hard drives will be encrypted.
Papers Containing Personal Data (e.g. contact details)	Paperwork containing personal data will not be left unattended and in sight. Tutors will ensure papers are stored securely to limit access.
Desktop Computers	All computers will be password protected and have a timed lock function when left unattended. Tutors must lock their workstations when leaving them unattended.
Staff Personal Devices	Staff are not permitted to use personal devices to access or store personal data relating to the company.
Sharing with Authorised Third Parties	When sharing data with authorised third parties, the school and staff will ensure data is handled securely and in compliance with GDPR.

8. Disposal of Data

Brilliant Coaching and Development ensures that records containing personal and/or sensitive data are disposed of safely and securely. Paper records due for disposal will be securely shredded either on site or by an approved third-party disposal service. If using a third party, the company must ensure the records are disposed of securely.

Digital records containing personal data will be deleted using the internal erasure procedure of the relevant software (e.g. Windows delete functions). It is the responsibility of individuals to delete personal data from devices once it is no longer relevant or if the device is to be passed on.

When disposing of sensitive personal data, the school will use a file-wiping utility to permanently remove sensitive data, preventing possible retrieval.

9. Compliance Monitoring

As data collection and processing evolves, Brilliant Coaching and Development maintains compliance through regular monitoring. The company director will regularly review data records to ensure they are relevant, necessary, and accurate. The director will monitor the compliance of roles outlined in this policy, impartially checking that responsibilities are fulfilled in accordance with the policy. Additionally, the director will oversee data sharing practices and the integrity and necessity of third-party data processing, as well as procedures for subject access requests (SAR) and data breaches, ensuring these procedures are correctly and promptly followed.

10. Data Breaches

Brilliant Coaching and Development takes all reasonable steps to ensure data handling and processing is safe and secure in line with GDPR. In the event of a data breach, the following procedure will be followed:

- Any potential or confirmed data breach must be reported initially to the company director.
- The director will investigate the breach to assess its severity.
- The director will log the outcome, including whether the breach needs to be reported, the cause and facts surrounding the breach, its effects, and the actions taken to minimise risk and prevent recurrence.
- If the director determines that the breach poses a significant threat to data subjects, they will report the breach to the ICO within 72 hours.
- The director will take action to minimise the impact of the breach, with support from relevant parties within the school.
- Upon receiving the ICO report, the director will act upon the ICO's recommendations.

Appendix: Data Processing Agreement (DPA)

Data Processing Agreement

This Data Processing Agreement ("DPA") is made between:

- The Academy Trust - Delta Academies Trust ("the Data Controller")
- Brilliant Coaching and Development ("the Data Processor")

Effective date: [Sept 2025]

1. Purpose of this Agreement

This DPA establishes the terms under which Brilliant Coaching and Development will process personal data on behalf of the Academy Trust. The primary objective is to ensure both parties comply with their obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Roles and Responsibilities

The Academy Trust serves as the Data Controller and is responsible for determining the purposes and means of processing personal data. Brilliant Coaching and Development acts as the Data Processor, carrying out the processing of personal data only in accordance with the written instructions provided by the Academy Trust.

3. Nature and Purpose of Processing

The processing of personal data under this agreement is intended to facilitate the delivery of tutoring, coaching, and mentoring services to students referred by the Academy Trust.

The nature of the processing includes accessing, storing, recording, and reporting relevant student information required to provide educational support services. Processing will occur for the duration of the agreement between both parties and for any additional period necessary to fulfill legal or safeguarding obligations regarding data retention.

4. Categories of Data and Data Subjects

Data subjects include students, their parents or guardians, and school staff who are involved in the provision of services.

The categories of personal data processed may include:

- Student initials or names (when required)
- Year group, subject, and learning objectives
- Session records or progress notes

- Contact information used for communication and coordination
- Safeguarding or wellbeing notes (if applicable and only when required)

Sensitive or special category data, such as medical, wellbeing, or safeguarding information, will only be processed when strictly necessary and with appropriate safeguards in place.

5. Data Processor Obligations

Brilliant Coaching and Development agrees to the following obligations:

1. Process personal data only upon receiving written instructions from the Academy Trust.
2. Ensure that all staff involved in handling personal data are properly trained and are bound by confidentiality requirements.
3. Implement suitable technical and organizational security measures to safeguard data from unauthorized access, loss, or disclosure.
4. Notify the Academy Trust without undue delay of any data breach or suspected breach.
5. Assist the Academy Trust in responding to data subject requests, such as those for access, correction, or deletion of personal data.
6. Delete or return personal data at the conclusion of the service, unless retention is legally required (for example, for safeguarding or financial records).
7. Maintain records of all processing activities as required by Article 30 of the UK GDPR.

6. Sub-Processors

Brilliant Coaching and Development may engage third-party service providers (sub-processors) to deliver elements of its services. Examples include:

- Microsoft Teams (for online tutoring sessions)
- GoDaddy (for website hosting)
- Accounting and payment systems (for invoicing purposes)

All sub-processors used are GDPR-compliant and are contractually obligated to adhere to equivalent data protection standards. The Academy Trust will be informed prior to the engagement of any new sub-processors.

7. Data Security

Data security measures implemented by Brilliant Coaching and Development include:

- Password-protected devices and encrypted storage solutions
- Use of secure online platforms, such as Microsoft Teams, for communication and tutoring sessions
- Restricting access to personal data based on a “need-to-know” principle
- Regular reviews of data security practices to ensure effectiveness and compliance

8. Data Breaches

In the event of a personal data breach, Brilliant Coaching and Development will:

- Notify the Academy Trust as soon as possible, and no later than 48 hours after the breach is discovered
- Provide comprehensive details regarding the breach, the data affected, and corrective measures taken
- Fully cooperate with the Academy Trust in managing any necessary notifications or remedial actions

9. Data Subject Rights

The Data Processor will assist the Academy Trust in responding to any requests from data subjects to exercise their rights under the UK GDPR, including requests for access, rectification, deletion, or restriction of processing of their personal data.

10. Termination and Data Return

Upon the completion or termination of the services provided:

- All personal data will be securely deleted or returned to the Academy Trust within 30 days, unless there is a legal requirement for retention
- Confirmation of the deletion of data will be provided to the Academy Trust upon request

11. Governing Law

This Agreement is governed by and construed according to the laws of England and Wales. Both parties agree to the exclusive jurisdiction of the English courts.

Signatures

For and on behalf of the Academy Trust	For and on behalf of Brilliant Coaching and Development
	S.Witts

July 2026

Review date July 2027