45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

Ibberson Tutoring Solutions takes data protection very seriously. As such, this policy outlines the measures the company will put in place to ensure the protection of all personal and sensitive data about staff, clients and students. This policy outlines a data protection by design culture within the company so that all collection, storage and processing of data, whether digital or on paper, is carried out lawfully in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

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

The data protection principles that the company must follow in order to be compliant with GDPR state that personal data must be:

- Processed lawfully and in a transparent manner;
- Collected for legitimate purposes;
- Relevant and limited to what is necessary in order to fulfil the purposes for which it is processed;
- Kept up to date;
- Stored for no longer than is necessary;
- Processed in a way that ensures it is appropriately secure.

This policy outlines how the company will comply with these principles.

Collecting personal data will be an inevitable part of the day-to-day business of Ibberson Tutoring Solutions. We will only collect personal data for specific, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data. To ensure that this data is handled and processed appropriately and with minimal risk, Ibberson Tutoring Solutions, as data controller, adheres to the guidelines outlined in this policy.

As with the collection of personal data, it is integral to the effective functioning of Ibberson Tutoring Solutions that personal data will need to be shared in certain circumstances. To ensure that personal data is shared lawfully, the following considerations must be taken into account.

45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

Scenario	Procedure
Regulatory bodies e.g. government agencies or healthcare	Before sharing personal data with regulatory bodies requesting access, the DPO will verify the identity of the body and investigate how they intend to use the data shared with them. Only when satisfied with the response will Ibberson Tutoring Solutions share any personal data.
Suppliers or Subcontractors Requiring Access to Personal Data	The DPO will assess all suppliers and subcontractors' ability to adhere to GDPR. All suppliers and subcontractors requiring access to personal data will read and follow the company's GDPR policy.
The Police	The police will only be able to request access to data with a relevant warrant.
Safeguarding concerns	All safe guarding concerns are discussed with the DSP who will then be required to relay this on to the relevant local authorities.

As part of GDPR, data subjects are entitled to make a request to any organisation to access personal information held about them. This is known as a subject access request (SAR). Ibberson Tutoring Solutions therefore needs to be reasonably prepared for such an eventuality by establishing the procedure outlined below.

NB: Personal or sensitive data about a child belongs to the child. However, if a child is deemed unable to understand their rights or the implications of a SAR, or is unable to give consent, a parent or guardian can make the request on their behalf.

Subject Access Request Procedure
1. All staff are trained to recognise a subject access request 2. Staff involved in responding to a SAR clearly understand the notion of the right to access. They also know when a SAR can be refused and how to act when refusing a SAR. 3. The company will use the education specific SAR form 4. Identification of the subject requesting access will be verified 5. The company aims to respond to all SARs within one month of submission 6. Upon receiving a valid SAR, the following procedure will be followed: The staff member who receives the written SAR refers this to a member of senior leadership A review of the SAR is carried out in order to establish the exact information requested The SAR is recorded in the company SAR log and reported to the DPO The DPO will send a response to the data subject to inform them that their SAR is being processed The information will be collated and the request responded to The record on the SAR log is marked as closed.

45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

Ibberson Tutoring Solutions recognises that photos, video and CCTV images of individuals will be part of the personal data processed by the school. As a result, the following measures are adhered to in order to ensure responsible handling and processing of such data.

CCTV
Ibberson Tutoring Solutions uses CCTV in various locations around the office building to keep staff, pupils and buildings safe. All CCTV data will be stored with our security company and not on site.

Photos and Video
Photos and videos taken within the company for public use are to be considered under GDPR. Any photo or video of recognisable individuals which the company wishes to publish for example, on the company webpage or social medial platforms, will only be published with prior written consent. Written consent will be obtained via email or written letter. Photographs and video captured by parents for personal use do not fall under the scope of GDPR.

At Ibberson Tutoring Solutions only data that is adequate, purposeful, necessary and limited to what is essential will be stored. The company will ensure that any stored data will be protected from unauthorised access and data breaches through the implantation of up to date and well-maintained security protocols. This will guarantee the confidentiality, integrity and availability of personal data. Confidentiality means that data will only be accessed by those who are authorised to access it. The integrity will be maintained through guaranteed accuracy and suitability of all data stored; inaccurate or unsuitable data will not be trained. Availability will be maintained, meaning those that are authorised to access the personal data are able to do so as and when required.

45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

Specific Data Type	Security Measures
Paper records	All paper records stored on site will be kept in a secure and locked location. Only those authorised to access the records will be granted access to the storage location.
Portable electronic devices e.g. laptops, iPads, phones	All portable devices will be password protected. In case of laptops the hard drives will be encrypted.
Papers containing personal data e.g. student records contact sheets registers/attendance charts feedback sheets	Any paperwork containing personal data will not be left unattended and in sight at any time. Tutors and other staff will ensure that any paper containing personal data will be suitably stored to limit access to the data.
Desktop computers within company	All computers used in the company are password protected and have a timed lock function if left unattended. Staff are will be required to lock their workstations when leaving them unattended at any time.
Staff personal devices	Staff will not be permitted to use personal devices to access or store any personal data relating to the school.
Sharing with authorised third parties	When required to share data with authorised third parties, the company and staff will make the necessary checks to guarantee it is handled securely and in line with GDPR.

For remote working to comply with GDPR, Ibberson Tutoring Solutions implements the following procedures:

- All staff laptops will have encrypted hard drives and will be password protected
- When working remotely and accessing the company's network, staff will use a secure password; this will prevent unauthorised access to company computer systems and networks
- Staff will only be able to use electronic devices provided by the company to work at home on any personal/sensitive data and/or access the company network
- Staff laptops will have up-to-date antivirus software installed to prevent any malicious or unauthorised access to company records, personal or sensitive data
- Staff are permitted to use personal or home Wi-Fi networks but are not permitted to use public Wi-Fi when working remotely. Public Wi-Fi security is not always strong enough to prevent a data breach
- All laptops provided by the company will be encrypted and password protected. If using a USB stick/portable hard drive to transport personal or sensitive data, this will also be encrypted.

Ibberson Tutoring Solutions will always ensure that records containing personal and/or sensitive data are disposed of safely and securely.

IBBERSON TUTORING SOLUTIONS

45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

For example, any paper records due to be disposed or will be shredded, either on site, or through an approved third-party disposal service. When using a third party, it is the company's responsibility to ensure that the company guarantees the records are disposed of securely.

Any digital records containing personal data will be deleted using the internal erasure procedure of the relevant software. For example, records stored on Apple laptops would be deleted using the Apple delete functions. It is up to individuals to make sure they have deleted personal data from devices once that data is no longer relevant, or the device is being passed on.

When disposing of sensitive data, the company will use a file-wiping utility to remove the sensitive data, preventing the possible retrieval if erased, using internal procedures.

As data collection and processing changes and updates, Ibberson Tutoring Solutions confirms continual compliance through compliance monitoring. The designated DPO will, as part of their role, undertake regular monitoring of data records held by the company, checking they are relevant, necessary and accurate. The DPO will monitor the compliance of the roles with their assigned responsibilities, impartially checking that these are carried out in accordance with the policy. The DPO will monitor who the school is sharing data with and the integrity and necessity of the third-party data processing. The DPO will monitor procedures for SAR and data breaches, ensuring these are followed correctly and in a timely manner.

At Ibberson Tutoring Solutions all reasonable action will be taken to keep data handling and processing safe and secure within GDPR. However, should a data breach occur, Ibberson Tutoring Solutions will be prepared to handle any such breach in the manner outlined below. Potential data breaches within a company context could be the loss of a USB device/portable hard drive containing pupil assessment data or an email containing sensitive personal data could be sent to an incorrect email address.

45 Fitzroy Street, London, W1T 6EB
+34 622879241
admin@ibbersontutoring.com

Ibberson Tutoring Solutions Procedure for Handling a Data Breach
• Any potential or confirmed data breach must be reported in the first instance to the DPO • Upon receiving notification of the data breach, the DPO must report this to the CEO and other Senior Leadership Team members • The DPO will investigate the data breach further to assess the severity of the breach • Once the assessment has been made the outcome will be logged by the DPO, whether the breach does or does not need reporting. The log will include the cause of the data breach and any facts surrounding the breach, the effects of the breach and the action taken to minimise risk and prevent a repeat occurrence • If the DPO determines that the data breach poses a significant threat to the data subject(s), they will report the breach to the ICO within 72 hours • The DPO will attempt to minimise the impact of the breach, supported by relevant parties within the company • Upon receiving the ICO report, the DPO will act upon the ICO's recommendations.