General Data Protection Regulation (GDPR)

Policy and Procedures

Reviewed and updates: [02.10 23]

Due for Review: [02.10.24]

Contents

1. Aims

Key Stage Tutoring takes data protection very seriously. As such, this policy outlines the measures the school will put in place to ensure the protection of all personal and sensitive data about staff, visitors, pupils and other individuals. This policy outlines a data protection by design culture within the school 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.

2. Legislation and Guidance

General Data Protection Regulation (GDPR) came into force in May 2018 as part of the Data Protection Act 2018 (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.

3. Definitions

Throughout this policy, the following terminology with the accompanying definitions will be used.

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 case of the school this could relate to 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	Relates to a set of special categories that should be treated with extra security. These categories are: • Racial or Ethnic Origin Data • Political Opinions • Religious or Philosophical Beliefs • Trade Union Membership • Genetic Data • Biometric Data
data controller	Any person, agency or authority who decides how and why data is processed. In the case of this policy the school is the data controller.
data processor	Any person, 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 of or access to personal data while stored, transmitted or being processed 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	Those who process personal data. They must protect data in accordance with this data protection policy.
data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.

4. Roles and Responsibilities

Key Stage Tutoring will follow the outline below for distribution of responsibilities in relation to GDPR within the school.

Role	Responsibility
Data Protection Officer (DPO)	The DPO will follow all necessary guidance outlined in this policy.
Tutors	The DPO will follow all necessary guidance outlined in this policy.

5. Data Protection Principles

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

- processed lawfully, fairly 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 school will comply with these principles.

6. Collecting Personal Data

Collecting personal data will be an inevitable part of the business of Key Stage Tutoring. We will only collect personal data for specific, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

To ensure that this data is handled and processed appropriately and with minimal risk, Key Stage Tutoring as data controller, adheres to the guidelines outlined below.

Scenario	Procedure
Pupil Contact Records	Relevant contact information will be collected when a responsible adult signs a pupil/student up for lessons. Contact information will be collected by online, password protected Google Docs Forms.
Pupil Progress Data	Relevant progress records/ assessment scores/ lesson notes will be kept about pupils/students. Lesson notes will be made online with OneNote documents. Notebooks will be shared with parents and only accessible via a shared link.
Special Educational Needs (SEN) Records	Relevant notes to be stored in a cloud storage system that is password protected.
Medical Information and Administration	Relevant notes to be stored in a cloud storage system that is password protected.
Safeguarding Records	Relevant notes to be stored in a cloud storage system that is password protected.

7. Sharing Personal Data

As with the collection of personal data, it is integral to the effective functioning of Key Stage Tutoring 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.

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 Key Stage Tutoring 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 school GDPR policy.
The Police	The police will only be able to request access to data with a relevant warrant.

8. Subject Access Request (SAR)

As part of GDPR, data subjects are entitled to make a request to any organisation, such as a school, to access personal data held about them. This is known as a subject access request (SAR). Key Stage Tutoring 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 should recognise a subject access request.
2) Staff involved in responding to a SAR should understand the notion of the right to access. They should know when a SAR can be refused and how to act when refusing a SAR.
3) The school will use the school specific SAR form. (See appendix 1)
4) Identification of the subject requesting access will be verified.
5) The school 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 the head of Key Stage Tutoring.
    - A review of the SAR is carried out in order to establish the exact information requested.
    - The SAR is recorded in the school 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.

9. Photos, Video, CCTV

Key Stage Tutoring 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

- Key Stage Tutoring may use CCTV in various locations around the school classroom/ grounds in order to keep staff, pupils and buildings safe.
- The school will endeavour to inform all members of staff, pupils, and visitors of where, when and how CCTV images are processed.
- All CCTV data will be stored for a period deemed reasonable for security purposes.

Photos and Video

- Photos and videos taken within school for public use are to be considered under GDPR.
- Any photo or video of recognisable individuals which the school wishes to publish for example, on the webpage will only be published with prior written consent. Written consent will be obtained from parents/caregivers.
- Photographs and video captured by parents for personal use do not fall under the scope of GDPR.

10. Data Retention - Security and Storage

At Key Stage Tutoring only data that is adequate, purposeful, necessary and limited to what is essential will be stored. The school will ensure that any stored data will be protected from unauthorised access and data breaches through the implementation 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 retained. Availability will be maintained, meaning those that are authorised to access the personal data are able to do so as and when required.

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.	All portable electronic devices will be password protected. In the case of laptops the hard drives will be encrypted.
papers containing personal data e.g. class lists contact sheets dinner registers	Any paperwork containing personal data will not be left unattended and in sight at any time. Teachers and other classroom staff will ensure that any paper containing personal data will be suitably stored to limit access to the data.
desktop computers within the school	All computers used in the school will be password protected and have a timed lock function when left unattended. Staff 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 school and staff will make the necessary checks to guarantee it is handled securely and in line with GDPR.

11. Staff Remote Working

For remote working to comply with GDPR, Key Stage Tutoring implements the following procedures:

- All staff laptops will have will be password protected. All documents will be kept in a cloud based storage system.
- When working remotely and accessing the school data, staff will use a secure password; this will prevent unauthorised access to school computer systems and networks.
- Staff will only be able to use electronic devices provided by the school to work at home on any personal/sensitive data and/or access the school data.
- Staff laptops will have appropriate antivirus software installed to prevent any malicious or unauthorised access to school 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 school will be password protected. If using a USB stick to transport personal or sensitive data, this will also be encrypted.

12. Disposal of Data

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

For example, any paper records due to be disposed of will be securely shredded, either on site, or through an approved third-party disposal service. When using a third party, it is the school'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 a Windows laptop would be deleted using the Windows 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 personal data, the school will use a file-wiping utility to remove the sensitive personal data, preventing the possible retrieval if erased, using internal procedures.

13. Compliance Monitoring

As data collection and processing changes and updates, Key Stage Tutoring confirms continual compliance through compliance monitoring. The designated DPO will, as part of their role, undertake regular monitoring of data records held by the school, checking they are relevant, necessary and accurate. The DPO will monitor the compliance of the roles outlined in this policy with their assigned responsibilities, impartially checking that these are carried out in accordance with 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.

14. Data Breaches

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

Key Stage Tutoring Procedure for Handling A Data Breach
• Any potential or confirmed data breach must be reported in the first instance to the DPO. • 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 school. • Upon receiving the ICO report, the DPO will act upon the ICO's recommendation.

15. Appendix 1

Subject Access Request Form

Title	
Surname	
First Name(s)	
Date of Birth	
Home Address	
Post Code	
Contact Telephone Number	
Email Address	
Relationship with the school	*Please circle:* Parent / Pupil / Member of staff / Governor / Volunteer / Other If other, please specify:
Identification provided To validate name and address	
Details of data request Please include as much information as possible about the data you are requesting. For example: your personal file, your child's progress data, emails sent between A and B and specific dates.	

I am requesting access to my own personal data, as detailed above. I confirm that I am the individual named above and the data I am requesting access to is my own personal data. I have supplied the information above to aid the subject access request and also to validate my identity. I have provided identification to prove my name and address.

Signature:_____ Date: _____

16. Appendix 2

Data Breach Log Form

Date of breach	
Date breach was discovered	
Cause of breach	
Description of the breach What happened? Who is involved? Other facts:	
Reported to ICO?	Yes ☐ No ☐
Date reported to ICO (If reported)	
All data subjects informed?	Yes ☐ No ☐
Remedial action	
Follow-up (if required)	
Breach reported by	
Date reported	
Report received by	