Winchmore Tutors Ltd (WT) collects and uses personal information about staff, pupils, tutors, parents and other individuals who come into contact WT. This information is gathered in order to enable it to run its business and provide tutoring and other associated educational activities. In addition, there may be a legal requirement to collect and use information to ensure that WT complies with its statutory obligations.

WT has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. WT also has a duty to issue a Fair Processing Notice which can be viewed on our website to all pupils/parents, clients and tutors. This summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.
Currently, the Registered Data Controller (RDC) for WT is Craig Varney – 01372 940809

Purpose
This policy is intended to ensure that personal information is dealt with (internally within WT) correctly and securely and in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?
Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

GDPR Principles
GDPR establishes six enforceable principles that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

General Statement

WT is committed to maintaining the above principles at all times. WT ensures that:

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Data is only processed where we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees (*including new starters and agents*) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their role and our business
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news and updates, to stay abreast of updates, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a **[Registered Data Controller/Responsible Person]** who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We provide clear lines of reporting and supervision with regards to data protection
- We store and destroy all personal information, in accordance with the data protection laws timeframes and requirements
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13 & 14 information disclosures
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security

Legal Basis for Processing *(Lawfulness*)

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the data protection laws and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information audit register and where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -***

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

Third-Party Processors

The Company utilise external processors for certain processing activities *(where applicable*). We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to****): -***

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Credit Reference Agencies
- Direct Marketing Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the data protection laws even when a process is handled by a third-party.

We have Service Level Agreements (SLAs) and contracts with each data processor which outlines: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to secure the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Company in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Company, all information necessary to demonstrate compliance with the obligations set out here and in the contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract

Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the RDC, or nominated representative.

Appendix 1

Winchmore Tutors
Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information
We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).
Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.
Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Actioning a subject access request
Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the **[Registered Data Controller/Compliance Officer]** as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

If there are concerns over the disclosure of information then additional advice should be sought.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, client, tutor or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

Please refer to our external ***Subject Access Request Procedures*** for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

The Right to Erasure
Also, known as *'The Right to be Forgotten'*, the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Company is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Data Retention & Erasure Policy for exact procedures on erasing data and complying with the Article 17 requirements.

Complaints
Complaints about the above procedures should be made to the RDC who will decide whether it is appropriate for the complaint to be dealt with in accordance with the WT complaints procedure.
Complaints which are not appropriate to be dealt with through the WT complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any enquires in relation to this policy, please contact - the Registered Data Controller for WT at rdc@winchmoretutors.com, who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 123 1113