**General Data Protection Regulation (GDPR) Policy and Procedure for Wendover Education and Wendover Online School**

1. Introduction

Wendover Education is made up of an online teaching provider, educational consultancy and student placement agency.

This policy supports the legal requirements of the UK General Data Protection Regulation which sits beside the amended Data Protection Act 2018 which places certain obligations on the Company, its staff and those who process data on our behalf. The EU GDPR was incorporated directly into UK law as the UKGDPR. We have students based in the EU and therefore the EUGDPR applies to services supplied to them. The EU approved adequacy decisions on 28 June 2021 which means data from the EU can flow as before in the majority of circumstances.

Data transferred from the EU to the UK for the purposes of UK immigration control is not included in the adequacy decision. Neither is data that would fall within the scope of the immigration exemption in the Data Protection Act (DPA) 2018.

Breach of this policy may result in the cessation of contract.

We do not have a formal Data Protection Officer. The members of staff responsible for data protection and their contact details are below.

- Sarah Bacon sarah.bacon@wendoverschool.com 07800 804041
- Rachel Smith rachel.smith@wendoverschool.com 07757 004104

This policy will be reviewed on an annual basis. It may, however, be amended in advance of such date in response to changes in future legislation.

The Company is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

Changes to data protection legislation shall be monitored and implemented to remain compliant with all requirements.

The principles of the Data Protection Act shall be applied to all data processed and shall be:

- Processed fairly, transparently and lawfully.
- Obtained only for lawful purposes, will not be further used in any manner incompatible with those original purposes.

- Accurate and kept up to date.
- Adequate, relevant, and limited to what is necessary to achieve the contractual and legal purposes of the company.
- Not kept for longer than is necessary for those purposes.
- Processed in accordance with the rights of data subjects under the DPA.
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- In the case of EU residents or citizens, data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

2. Organisational Scope

This GDPR Policy is a corporate policy and applies to former, current, and potential employees and associates of Wendover Education. Moreover, this policy will form part of an agreement with any organisation which may be engaged to process personal data on behalf of the Company in the future.

We are a data controller and data is processed by our staff in the UK, however, for the purposes of IT platform hosting and maintenance this information is located on MS platforms such as SharePoint. We will not collect any information from you that we do not need in order to provide and oversee our services to you.

We have conducted an information audit and we currently collect and process the following information:

- Personal identifiers, contacts, and characteristics i.e. full name, DOB, gender, nationality, visa Biometric Residence Permit, passport and contact details of parents, schools, students, employees, contractors and agents.
- Personal images for identification. Normally taken from a Passport provided directly by the subject.
- Other files relevant to the provision of our service for example boarding cards for flights.
- Medical, including SEND information.
- Cultural data.
- Financial, including invoice and pricings.
- Academic data such as school reports, notifications, and disciplinary matters.
- Lifestyle choices such as likes, dislikes, sports, hobbies.
- Employee, contractors /consultants vetting and recruiting information.
- Proof of Right to Work (RTW) in the UK such as a UK Passport or other documentation such as BRP, Home office letter of indefinite right to remain or a visa vignette.
- Proof of Identity and address documentation for DBS processing. Note: Only the RTW document is retained the remainder is deleted after DBS processing is complete.
- Photocopies of Passports and other documents needed to prove the Right To work in the UK are held on an external hard drive separated from SharePoint and held at rest (offline) in locked containers.

Definitions

This section includes all necessary definitions of terms used in the policy which are not in everyday usage or where there is a need to be precise.

Consent
Consent means offering people genuine choice and control over how we use their data. Consent must be freely and explicitly given to be valid under GDPR.

Data subject
Data subject means "an individual who is the subject of personal data". A data subject must be a living individual.

Information Commissioner's Office (ICO)
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforce the law regarding information compliance legislation. The ICO has the power to impose substantial fines of up to £17.5 million or 4% of our total worldwide turnover, whichever is higher.

Lawful processing for legitimate interests
Processing is necessary for the purposes of the legitimate interests pursued by the controller 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.

Personal data
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach
Personal information data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. We are legally obliged to report breaches that are likely to result in a risk to the rights and freedoms of individuals to the ICO and individuals will have to be notified directly by the Company.

Processing of personal data
Processing, in relation to information or data, means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,

- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

Records disposal
The Company will retain records for only as long as they are needed and then, when they are no longer needed, destroy them in an appropriate manner, e.g. by permanent and irretrievable deletion.

Retention period
The periods of time, varying from a few months to permanency, during which a record must be maintained by the Company. This is usually determined by statute, legal, regulatory, or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention.

Company community
For the purposes of this Policy this includes core staff, students, contractors, teachers and others with a direct impact on or responsibility to the Company.

How we get the information and why we have it
The personal information we process is provided to us directly by parents on registration or by students of 13 years or older and by employees or contractors during recruiting and vetting procedures and to prove identity for the Disclosure and Barring Service (DBS).

## 3. Policy Statement

The Company and individual members of the Company community are expected to abide by the laws in force in this area. All Company staff and contractors processing data on behalf of the Company are responsible for any breaches of such legislation.

## 4. Key Principles

4.1. Wendover Education is strongly committed to complying with its legal obligations regarding the protection of personal data and privacy of individuals.

4.2. This Policy and procedure sets out the minimum requirements for data processing by the Company to protect the rights of data subjects.

4.3. Wendover Education needs to keep and process certain information about its employees, contractors, students, and others to allow it to comply with legal obligations, and to operate in an effective and efficient manner.

4.4. To comply with the existing Data Protection Act requirements and the General Data Protection Regulation, personal information must be collected and used fairly, stored

safely and not disclosed to any other person unlawfully. To do this, Wendover Education staff, students and contractors must comply with the Principles and protections set out in the Data Protection Act currently in force, UK GDPR and reiterated in this Policy.

4.5. Wendover Education must only retain personal data in line with the guidance set out in the Wendover Education Retention Schedule. This document provides advice as to retention periods suitable for types of records prior to any disposal decisions being made.

4.6. All processing of personal data under the GDPR needs to have a legal basis, and Wendover Education must be able to demonstrate, to the ICO or to the individual, this basis.

4.7. It is important to determine the legal basis for processing as under the GDPR this has an influence on an individual's rights. For example, consent provides individuals with stronger rights such as having data deleted.

4.8. Processing Conditions

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject.
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the purposes of the legitimate interests of Wendover Education or the legitimate interests of a third party.

4.9. The DPA / GDPR introduces a duty on Wendover Education to report serious data breaches to the ICO, and often to the individuals affected. A notifiable breach must be reported to the ICO within 72 hours of Wendover Education becoming aware of it as well as, when appropriate, notification to the data subject within the same tight timescale.

4.10. Fines have increased and the maximum fines can be up to £17.5 million or 4% of our total worldwide turnover, whichever is higher, for a breach, depending on the severity, scale, or impact of the breach. It is not simply a numbers game, the loss of hundreds of minor pieces of personal information might incur a smaller fine than a case where Wendover Education loses the sensitive personal health information of one individual.

4.11. Failure to report a breach can also result in fines for Wendover Education and potentially for the individual who has committed the breach. Wendover Education requires all incidents and breaches to be reported so we can assess and reduce the risks and where possible prevent incidents from becoming serious breaches.

4.12. All employees and contracted teachers must undertake the Wendover Education GDPR training or prove they have already done so within the year of employment.

5. Procedure

Data Held and Processed by Wendover Education

5.1. Wendover Education will use and otherwise process records of personal information relating to data subjects relevant to the effective functions and operation of its role as an online education provider and employer.

5.2. Where required, Wendover Education will obtain freely given consent for all types of personal data processing except that specifically exempted by the Regulation.

5.3. The use of the information and retention of the personal data will be specifically defined within Wendover Education's central personal data processing log.

5.4. All staff, contractors, students, and other data subjects about whom personal information is held may have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Some of these rights may be restricted depending on the lawful basis Wendover Education is relying on for the processing and can also affect which rights are available to individuals. The ICO provides the following examples:

| | Right to erasure | Right to portability | Right to object |
|---|---|---|---|
| Consent | Y | Y | N (but right to withdraw consent) |
| Contract | Y | Y | N |
| Legal obligation | N | N | N |
| Vital interests | Y | N | N |
| Legitimate interests | Y | N | Y |

5.5. This adds to the existing rights previously in place for data subjects which include a person's right to know:

- what information Wendover Education holds and processes about them
- why the information is held and processed

- details of whom the information might be shared with
- know how to gain access to such information
- know that it is up to date
- know what Wendover Education is doing to comply with its obligations under the Data Protection Act or other relevant legislation

6. Responsibilities of Staff in Relation to their own Data

6.1. All staff or consultants are responsible for:
- Checking that any personal data that they provide to Wendover Education is accurate and up to date; they are requested to check this periodically, informing Wendover Education of any changes or errors in the information held.

7. Responsibilities of Students in Relation to their own Data

7.1. Parents, legal guardians, and students over the age of 13 will, at the time of registration, be required to agree to the use of essential personal data for Wendover Education administrative purposes, which will be clearly specified.

7.2. Parents, legal guardians, and students must assist Wendover Education in ensuring the accuracy of the personal data as provided to Wendover Education and that the information is up to date.

8. Basic responsibilities on staff for Data Security of Third-Party Personal data

8.1. Wendover Education has a legal requirement to ensure that data is held securely, and this includes the provision that access, and disclosure of personal data, should be restricted to those who have a legitimate, authorised purpose.

8.2. Staff and consultants/teachers have a responsibility for using and otherwise processing personal data in compliance with this Policy and more specifically operating under the terms of the relevant Data Protection legislation.

8.3. Therefore, all Wendover Education staff and associates are responsible for ensuring that:
- personal information is not disclosed by them either orally or in writing, to any unauthorised third party.
- they do not access any personal data which is not necessary for carrying out their work/teaching.
- personal data in paper format is kept in a secure place when not being processed.

9. Responsibilities on students for Data Security of Third-Party Personal data

9.1. Students and teachers may need to process personal information for lesson projects or surveys but the data subject should be informed of details such as why the data is being collected and how long it will be retained for.

10. Right of Access to Information

10.1. The ICO provides information regarding valid requests for a data subject to access their personal data (A Subject Access Request or SAR).

1.1.1. An individual can make a SAR verbally or in writing including on social media.

1.1.2. If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data. The GDPR provides for a data subject to have the right of erasure of personal data.

11. Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, which are:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent (if consent has provided the justification for processing).

All data subjects have the right to apply for access to any personal data that is being kept by about them either digitally or on paper files. Any person who wishes to exercise this right should make a written request to Wendover Education. Wendover Education cannot charge any fee or disbursement for such a service.

All requesters will be asked to include proof of identity and no response will be sent until such proofs have been provided. Wendover Education will ensure that requests for information are responded to within the statutory month period.

12 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

However, the right to data portability only applies:

- to personal data an individual has provided to Wendover Education.

- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

## 13 Right to Object

Individuals have the right to object to:

- processing based on legitimate interests (including profiling).
- data used for unauthorised marketing purposes.
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed (i.e. in breach of the GDPR).
- the personal data must be erased to comply with a legal obligation.

Individuals must have an objection on "grounds relating to his or her particular situation". Therefore, Wendover Education will have to stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or:

Publication of Wendover Education Information

There may be Information that is already in the public domain, for example Wendover Education web pages.

## 14 Personal Data Breach

All personal data breaches should be reported to the Officer responsible for Data Protection who will make a judgement on the severity of the breach.

Breaches involving large losses or misuses of personal data or any involving 'sensitive' personal data will be reported to the Officer responsible for Data Protection to investigate more fully. To help assess the seriousness of a breach please refer to Appendix 2 and Appendix 3.

Data breaches may include hacking by external actors or misuse of Wendover Education office or remote working computers.

In the event of a theft of data or a device containing data when away from Wendover Education, the police should also be notified of the theft.

## 15 Actions to be taken in Response to a Personal Data Breach

As soon as a breach has been detected or is suspected the following steps should be taken:

- An immediate attempt should be made by the line manager to recover any personal data lost or misplaced.

- Liaise with those involved with the breach to prevent the further worsening of any breach.
- Consideration should be given as to whether to notify those affected by any such breach. Wendover Education is strongly in favour of notifying those affected but in any event those who may suffer damage (including reputational damage), or loss should always be informed.
- Steps should be taken to review processes and procedures to reduce the risk of further breaches happening again.
- Systems and procedures will be reviewed by the responsible Officer 3 months after the breach to make sure processes have been made more robust.
- Where relevant, those affected should be informed of the steps that have been taken to recover their personal data and reviews that have started to prevent issues happening in the future.
- Staff or associates responsible for major breaches or repeat minor breaches will be required to undertake remedial Data Protection training.
- In the case of serious breaches, deliberate breaches, or repeated breaches after training, Wendover Education will review the employment status of the individual concerned.
- In the case of serious breaches, the Wendover Education Data Protection Officer will be legally obliged to report such a breach to the ICO. This may result in fines for Wendover Education and for those committing major breaches.

The responsible Officer will retain records of all serious breaches.

## 16 Data Disposal

Wendover Education recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. Data held on devices are to be permanently and irretrievably deleted. Company issued devices have 'File Shredder' installed which will delete irretrievably. Data held on other devices such as Teachers' own personal PC must also be deleted. The Company recommends three free apps: File Shredder, Eraser, and Freeraser.

Time expired devices, thumb drives, CDs, tape, or other electronics no longer required shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. Paper records will be destroyed by fire on company property by the officer responsible for Data Protection.

Disposal of IT assets holding data shall follow ICO guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/

**Policy review**

This policy is designed to set good practice standards. However, Wendover Education recognises that best practice develops over time and, as such, will update it regularly in light of experience and as a result of changes in legislation or its own internal organisation and policies. As with all Wendover policies, this policy will be reviewed according to our comprehensive policy review calendar.

Date policy reviewed: August 2024

Date of next review: March 2025

**References**

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents?uri=CELEX%3A32016R0679&from=EN

UK GDPR guidance and resources
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Data protection for the public
https://ico.org.uk/for-the-public/

Self-assessment for data breaches
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

**Appendix 1: Examples of incidents which should be investigated**

Investigating parties should use the Self-assessment for data breaches tool provided by the ICO at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

This will not be a complete list but is designed to provide advice as to potential breaches that may occur.

- Sending emails or correspondence containing personal data to the wrong recipient.
- Sending non-essential personal data to otherwise valid recipients (for example including a string containing health details to all recipients when only one has rights to see it).
- Personal data received in error.
- Failure to secure access to Wendover Education devices, including incorrect allocation of permissions or sharing passwords, which result in unauthorised access to personal data.
- Misuse of Wendover Education computer systems to access personal details where there is no business purpose to do so
- Loss or theft of any Wendover Education-owned data storage device regardless of the data it contains e.g., laptop, PC, USB/pen drive, iPad, or other removable device.

**Appendix 2: Points for Investigating Staff to Consider**

- What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
- How did the breach occur?
- What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number)
- How many individuals or records are involved?
- If the breach involved personal data, who are the individuals?
- What has happened to the data?
- Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
- Were there any protections in place? (e.g. Encryption)
- What are the potential adverse consequences for individuals or Wendover Education? How serious or substantial are they and how likely are they to occur?
- What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
- What processes/systems are affected and how? (e.g. web page taken offline, access to database restricted)

**Appendix 3: Breach log template**

Completed forms to be retained by the Data Protection Officer.

| | Questions | Answers |
|---|---|---|
| 1 | When did the breach occur? | |
| 2 | When and how was it reported? By whom? | |
| 3 | What are the personal data affected? | |
| 4 | How many people have been affected? | |
| 5 | Where are the data now and how many people with no rights to access it have seen it? | |
| 6 | What has been done to recover the data? | |
| 7 | What policies or procedures have been put in place or amended to stop a recurrence of this breach? | |
| 8 | What training/ awareness raising measures have been taken in the light of this breach? | |
| 9 | Has this happened before? | |
| 10 | 3-month review to evaluate the impact of training and measures taken completed? | |