# Data Protection Policy

| | |
|---|---|
| Company name: | Vision for Education / ABC Teachers / Smart Teachers (part of Edwin) |
| Document | Data Protection Policy |
| Topic: | Data Protection |
| Date: | September 2025 |
| Version: | 11 |

## Contents


1. Introduction
2. General Guidance
3. Key Definitions
4. Data Protection Principles
5. Lawful Basis for Processing
6. Rights of the Data Subject
    - Receiving a Request from an Individual
7. Data Controller or Data Processor
8. Records of Processing Activities
9. Data Protection by Design and Default
    - When to Complete a Data Protection Impact Assessment (DPIA)
    - Procedure for Completing a DPIA
10. Security of Processing
11. Processing Special Categories of Personal Data
12. Safeguarding and Data Retention
13. Sending Electronic Marketing Messages to Individuals
14. Restricted Transfers of Personal Data Outside of the EEA
15. Breach Notifications
16. Incidents
17. Training
18. Contacting Your Data Protection Team

# Data Protection Policy

## 1. Introduction

This policy sets out the requirements applicable to the processing of personal data in Vision for Education, ABC Teachers and Smart Teachers. It has been written with consideration of all currently applicable privacy laws including the Data Protection Act 2018, the United Kingdom Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communication Regulations 2003.

When we process personal data we must always consider how we will be **transparent** with individuals whose personal data we process and **accountable** for the processing which we will carry out on that personal data.

This policy is applicable to all personal data processed within Vision for Education, ABC Teachers and Smart Teachers.

**The latest version of this policy is available at all times on our websites.**

## 2. General Guidance

- Whenever using personal data, it should be treated with the utmost confidentiality at all times.
- Continually understand what personal data you process and the reasons for processing it. If we are collecting data we do not use, this should be escalated to the **Data Protection Coordinator**.
- Before you start collecting new personal data, or start using personal data for a different reason than it was collected for, understand the privacy implications of this by carrying out a formal assessment.
- If you receive a request from an individual asking to enforce one of their Data Subject Rights, contact our Data Protection Coordinator immediately.
- If you think you have discovered a personal data breach or have any concerns regarding the use of personal data in the organisation, report these immediately to the Data Protection Coordinator.
- If you are unsure about what you should be doing with personal data, ask for guidance.

## 3. Key Definitions

To understand the requirements of this policy, it is important that all individuals understand the following key terminology.

### 1. Personal Data

Any information which relates to an identifiable individual. Including their basic identifiers and contact details, identification numbers or references, information about their location, behaviour or physiology and all online identifiers.

### 2. Data Subject (individual)

The person about whom personal data relates to. Within this document they will be referred to as the **'individual'**.

### 3. Processing

Any operation or set of operations that is performed on personal data. This includes collection, storage and organisation, use, disclosure and alteration, restriction, erasure and destruction.

### 4. Controller

This is the term used to define the organisation which, either alone or in conjunction with another, decides how personal data will be used.

### 5. Processor

This is the term used to define an organisation who processes personal data on behalf of a controller.

### 6. Special Category Personal Data

Where personal data is of a sensitive nature, controllers and processors must hold it in the highest regard for protection. The special categories of personal data include data relating to an individual's:

i. Ethnicity, race, religious or philosophical beliefs
ii. Political opinions or trade union membership
iii. Genetic data and biometric data which will be used for identification purposes
iv. Mental or physical health
v. Sex life or sexual orientation
vi. Criminal convictions or offences

### 7. Data Protection Coordinator

This is the individual who is responsible for providing data protection information and advice as well as monitoring compliance with all relevant privacy law. Our Data Protection Coordinator is supported by Evalian, a third party organisation which provides outsourced Data Protection Officer services. The Data Protection Coordinator will liaise with Evalian and escalate queries to them as necessary.

## 4. Data Protection Principles

Since the earliest Data Protection Law, key principles have defined and directed how personal data should be processed. Under UK GDPR we have 6 core principles underpinned by the principle of **accountability.**

### Accountability

The principle of accountability should be seen as underpinning everything which we do with personal data. This means that we should be able to consistently demonstrate how we process all personal data in compliance with the 6 Data Protection Principles.

The 6 Data Protection Principles are:

### 1. Lawfulness, fairness and transparency

Personal data must be processed in a lawful, fair and transparent manner in relation to the individual.

### 2. Purpose limitation

Personal data must be collected for specific, explicit and legitimate purposes. We should not process personal data in a manner that is incompatible with those original purposes.

### 3. Data minimisation

When collecting personal data it must be adequate, relevant and limited to what is necessary in relation t o the purpose it is being collected for.

### 4. Accuracy

We must take reasonable steps to ensure the personal data we process is as accurate and up-to-date as possible. If personal data is incorrect or inaccurate it should be corrected, completed or erased.

### 5. Storage limitation

Personal data should only be kept for as long as is necessary for the purpose it is being processed for.

### 6. Integrity and confidentiality

Personal data should be processed in a way that ensures appropriate security against unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## 5. Lawful Basis for Processing

Whenever we process personal data, we must do so in a lawful manner. Each processing activity we undertake must have a lawful basis for processing. There are six lawful bases for processing, each basis is equal and should be assigned on a processing-by-processing basis. The six lawful bases for processing are as follows:

1. The individual has given their **consent** to one or more processing activities.
2. The processing of personal data is required for the performance of or entrance into a **contract** with the individual.
3. The controller must process the individual's personal data to comply with a **legal obligation**.
4. Processing is necessary for the purposes of the controller or a third party's **legitimate interest** where those interests are not compatible with the rights and freedoms of the individual.
5. Processing is necessary in order to protect the **vital interests** essential in the protection of the individual or another individual's life.
6. Processing is necessary for performing a task in the **public interest** or in the exercise of an official appointment.

At Vision for Education, ABC Teachers and Smart Teachers the majority of our processing is on the basis of the second lawful basis, performance of or entrance into a contract with a data subject.

We will only send direct email marketing messages to individuals on the basis of consent. There are no instances where we will use our legitimate interests, also known as a soft opt-in, to undertake direct email marketing messages to individuals. All consents are mastered and amendable via Salesforce.

Where we are using Legitimate Interest as the basis for processing data, a Legitimate Interest Assessment will be completed and reviewed annually.

We record the lawful basis for processing alongside each activity in our Record of Processing Activities (ROPA) documented on spreadsheets stored in SharePoint.

Where special category personal data is processed, the organisation must have a further basis to process this personal data.

To understand what to do when you are processing special category personal data, please see **Section 11** of this policy.

## 6. Rights of the Data Subject

Controllers and processors are expected to support and provide mechanisms for individuals to uphold their Data Subject Rights. Individuals have 8 core data subject rights, but they are not all absolute rights. The applicability of individuals' data subject rights depends on factors such as the Lawful Basis for processing and the Data Protection Principles.

Individuals have the following data subject rights:

- To be **informed** about how their personal data is used.
- **Access** to their personal data.
- **Rectification** or completion of their personal data.
- **Erasure** of their personal data.
- **Restrict** how their personal data is processed.
- **Port** their personal data to another controller.
- **Object** to the use of their personal data.
- Rights relating to use of **automated decision making**, including profiling, using their personal data.

When a data subject makes a request exercising one or more of their rights, we must respond to that request within one month. In exceptional circumstances this can be extended.

The Data Protection Coordinator will follow the Data Subject Request Process. Where individuals have questions about their process, the Data Protection Coordinator should be the first point of contact.

The Data Protection Coordinator will maintain accountability for the requests they are processing by recording them in the specific software we utilise for tracking Data Subject Access Requests.

### Receiving a Request from an Individual

Any individual can make a request asking us to uphold one of their Data Subject Rights defined above.

These requests do not need to be in writing so staff need to be aware that a request could be received in person, online, by email, on the phone, via social media or in writing. If you are unsure whether an individual is making a request in line with their Data Subject Rights you should contact the Data Protection Coordinator immediately.

All requests received from individuals should be passed on to the Data Protection Coordinator using the inbox designated in **Section 16**.

## 7. Data Controller or Data Processor

The organisation has different responsibilities where we act as a controller compared to when we act as a processor. We are always obliged to understand what personal data we process regardless of whether we decide how that data is processed or whether another organisation makes that decision.

When a new third party is contracted, or we are contracted to a third party, we must maintain a record of this relationship along with information about the processing activities which we will undertake in the course of that relationship. This is called a Record of Processing Activities (ROPA). More information aboutthis can be found in **Section 8** of this policy. Prior to the onboarding of any new third party that will process personal data, the Data Protection Coordinator should be made aware.

Any new third parties that are onboarded will have their Data Processing Agreements or equivalent reviewed by our solicitors where necessary. These agreements will be stored alongside their main terms and other associated documentation on SharePoint. Access to these documents will be on a strict need-to- know basis.

Unless you have been cleared to do so, no employee should sign a Data Processing Agreement or similar without agreement from the Data Protection Coordinator.

## 8. Records of Processing Activities

All organisations processing personal data on a permanent basis are legally required to maintain a Record of Processing Activities (ROPA). This is a living document which should change and evolve as we add, amend or cease processing activities. The ICO requires that this record is granular and extensive which means every operational unit must be involved in its creation and maintenance.

All departments are required to understand the processing activities they undertake and inform the Data Protection Coordinator of any changes.

The organisation's ROPA is stored on spreadsheets in SharePoint and this is maintained by the Data Protection Coordinator. The Data Protection Coordinator is responsible for the upkeep and accuracy of the ROPA.

### New Vendor Onboarding Procedure

Vision for Education, ABC Teachers and Smart Teachers are committed to working only with reputable suppliers who work towards compliance with the standards of our code of conduct and abide by all applicable national and local laws and regulations in the markets where they operate.

When engaging with a new supplier, the process as detailed in our New Supplier Procedure must be followed to ensure that they have met our requirements and standards. Should the work that is going to be carried out by the supplier involve personal data, a GDPR Supplier Due Diligence Questionnaire should be completed by the supplier and sent to the Data Protection Coordinator who will review this document in conjunction with our DPO. The Data Protection Coordinator will also assess whether a Data Protection Impact Assessment (DPIA) should be completed and will liaise with our solicitors regarding data provisions in the contract and whether an additional Data Processing Agreement is necessary.

The following documents have been created to support this process and staff can find these on the Hub:

- New Supplier Procedure
- New Supplier Questionnaire
- Supplier Code of Conduct
- GDPR Supplier Due Diligence Questionnaire
- Data Protection Impact Assessment
- Third Party Processing Agreement (Data Processing Agreement)
- New Supplier Checklist

## 9. Data Protection by Design and Default

Data Protection by design and default is underpinned by an understanding of the risk apparent to individuals by processing their personal data. Before a new processing activity is undertaken, the organisation should understand how the data protection principles, security and data subject rights will be upheld. By understanding how this will be actioned, the organisation will design new processing activities with sufficient safeguards, protection and security implemented as standard.

This approach can be achieved in many ways, from designing systems with the highest levels of security as standard, getting assurances from third parties regarding their compliance, and risk assessing new technologies prior to their use.

A vital tool in implementing data protection by design and by default is a risk assessment called a Data Protection Impact Assessment, or DPIA.

The following procedures should be followed by the Data Protection Coordinator to assess the need and carry out a DPIA.

### When to complete a Data Protection Impact Assessment (DPIA)

Although not required for every processing activity, when a type of processing is likely to result in a high risk to the rights and freedoms of individuals, a DPIA shall be carried out before processing begins.

A DPIA is deemed to be required where a new processing activity will include at least two of the following 12 actions:

1. Systematic and extensive profiling or automated decision-making to make significant decisions about people.
2. Process will include special category data or criminal offence data on a large scale.
3. Systematic monitoring of a publicly accessible place on a large scale.

4. The use of new technologies or applications.
5. The use of profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
6. The carrying out of profiling on a large scale.
7. The processing of biometric or genetic data.
8. The combination, comparison or matching of data from multiple sources.
9. Processing of personal data without providing a privacy notice directly to the individual.
10. Processing of personal data in a way which will involve tracking individuals' online or offline location or behaviours.
11. The processing of children's personal data for profiling or automated decision-making or for marketing purposes, or to offer online services directly to them.
12. The processing of personal data which could result in a risk of physical harm in the event of a security breach.

Should a processing activity fulfil two of the above actions, the Data Protection Coordinator should be alerted so that a DPIA can be activated.

## Procedure for Completing a DPIA

Once it has been established that a DPIA is required, the Data Protection Coordinator will complete the DPIA template (the **DPIA template** on the Hub should be used). They will consult the IT department, any relevant processors and any other staff relevant to the project. Legal advice may also be sought where necessary. The DPIA should be completed as early as possible and should run alongside the planning and development process of the project. The following steps should be completed:

1. Description of the processing
    - **Nature of the processing** – what we plan to do with the data
    - **Scope of the processing** – what the processing covers
    - **Purpose of the processing** – why we want to process the data
2. Consider consultation
    - Do we need to design a consultation process to seek the views of the individuals whose data we will be processing?
    - If a data processor is involved, conduct a contract review in line with Article 28 to ensure that the contract is sufficient
    - Do we need to consult anyone else? e.g. data processor, IT manager, Chief Information Officer, legal advice, etc.
3. Assess necessity and proportionality
    - Do our plans help to achieve our purpose?
    - Is there any other reasonable way to achieve the same result?
4. Identify and assess risks
    - Consider the potential impact on individuals and any harm or damage the process may cause and log as risks
5. Identify measures to mitigate the risks
    - For each risk identified, record source and consider options for reducing the risk
6. Sign off and record outcomes
    - Record additional measures, whether risks have been eliminated, reduced or accepted, overall level of residual risk, whether we need to consult the ICO.

Where high-level risk cannot be sufficiently mitigated, the ICO should be consulted.

For further information, consult **ICO How to complete a DPIA**.

The DPIA should be integrated into the project plans, reviewed annually and kept under review throughout the duration of the project and amended accordingly.

## 10. Security of Processing

The level of security required shall be applied, and maintained, based on the level of risk posed by the processing activity.

The minimum standard of security shall be the level set out in the Information Security Policies (internal document).

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

As any approved codes of conduct or certifications are developed and approved by national or continental supervisory authorities, the application of these mechanisms shall be assessed and where relevant approved by the Chief Information Officer.

## 11. Processing Special Categories of Personal Data

The processing of personal data which reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, or data relating to criminal offences or convictions is prohibited unless an exemption applies. The Data Protection Act 2018 provides specific details regarding the exemptions and where they apply.

Should your department be processing, or planning on processing, special category personal data, the Data Protection Coordinator should be alerted.

## 12. Safeguarding and Data Retention

All information regarding safeguarding allegations, incidents and outcomes will be stored on the candidate file. This information will be retained under safeguarding lawful legitimate interest and shared accordingly where required in the interest of safeguarding children, young people and vulnerable adults.

Information regarding substantiated outcomes which meet the harm threshold will be included on outgoing references indefinitely.

Information regarding substantiated outcomes which do not meet the harm threshold will be including on outgoing references and will be shared with all future placement schools where relevant, and for three years after they cease to work with the company.

Information regarding allegations which are found to be unsubstantiated, unfounded or malicious will n o t be shared.

All information relating to incidents and allegations will be retained on the candidate file in accordance with our Data Retention Policy (internal document).

## 13. Sending Electronic Marketing Messages to Individuals

An electronic communication is any information sent between us and a data subject over a phone line or internet connection. This includes phone calls, text messages, video messages, emails and internet messaging.

If an individual has opted out of a particular form of communication as specified on their Contact Preference on Salesforce, we must adhere to this. Staff must use the 'remove and send' feature when sending emails and select 'No' on the 'Send to opt-out members' section when sending an SMS.

Where we rely on consent to process any personal information, consent may be revoked at any time. Marketing templates created by the Marketing team will include the option for recipients to update their contact preferences / unsubscribe. Vision for Education, ABC Teachers and Smart Teachers may use a third-party supplier to conduct its marketing communications.

Should an individual with pre-existing preferences approach any entity within Vision for Education, ABC Teachers and Smart Teachers regarding work, their marketing preferences will be re-established during the registration process.

If any marketing communications have been sent in error, or against preferences, please let the Data Protection Coordinator (dpo@edwin.group) know promptly.

## 14. Restricted Transfers of Personal Data Outside of the UK

A transfer of personal data to a country outside of the UK can only take place under limited circumstances. A transfer of personal data outside of the UK is deemed a restricted transfer where:

1. Personal data is sent, or made accessible, to a recipient to whom the UK GDPR does not apply; AND
2. The recipient is a separate organisation or individual. The recipient cannot be an employee of the company but can be a company within the same group.

A transfer is not the same as transit, where personal data is just electronically routed via a non-EEA country and the personal data is from one EEA country to another; no transfer is deemed to have taken place.

In any event that a processing activity may include the transfer of personal data outside of the UK, the Data Protection Coordinator should be alerted.

## 15. Breach Notification

A personal data breach is an event where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure or access to personal data.

If you think you have discovered a personal data breach, you should raise this immediately with your line manager and the Data Protection Coordinator.

All personal data breaches should be reported internally only. Where necessary, the Data Protection Coordinator will liaise with the DPO around informing the ICO of a breach.

## 16. Incidents

If, during the performance of your job, you are made aware of a breach of this policy, please report the incident via email to the Data Protection Coordinator.

## 17. Training

Internal staff will receive Data Protection training during induction and annually thereafter. All candidates have access to Data Protection training and where required this will be mandated.

## 18. Contacting Your Data Protection Team

Should you have a specific question relating to this policy, please address it to the Data Protection Coordinator at dpo@edwin.group.