Data Protection Policy

Contents

1. Introduction 2
2. General Guidance 2
3. Key Definitions 2
4. Data Protection Principles 3
5. Lawful Basis for processing 3
6. Rights of the Data Subject 4
   Receiving a request from an individual 4
7. Data Controller or Data Processor? 4
8. Records of Processing Activities 5
9. Data Protection by design and by default 5
   When to complete a Data Protection Impact Assessment (DPIA) 6
10. Security of Processing 7
11. Processing special categories of personal data 7
12. Safeguarding and Data Retention 7
13. Sending electronic marketing messages to individuals 7
14. Restricted transfers of personal data outside of the EEA 8
15. Breach notification 8
16. Incidents 8
17. Contacting your Data Protection Team 8

1. Introduction

This policy sets out the requirements applicable to the processing of personal data in the The Edwin Group. It has been written with consideration all currently applicable privacy law including the Data Protection Act 2018, the United Kingdom General 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.

The policy is applicable to all personal data processed within the Group.

The latest version of this policy is available at all times on The Hub.

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 our Data Protection Lead (DPL) - Jo Betteley.
- 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 your Data Champion immediately.
- If you think you may have discovered a personal data breach or have any concerns regarding the use of personal data in the organisation, report these immediately to our DPL - Jo Betteley.
- 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**
   a. 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)**
   a. The person about whom personal data relates to. Within this document they will be referred to as the **'individual'**
3. **Processing**
   a. 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**
   a. 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**
   a. This is the term used to define an organisation who processes personal data on behalf of a controller.
6. **Special Category Personal Data**
   a. Where personal data is of a sensitive nature, controllers and processors must hold it in the highest for protection. The special categories or 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 Officer (DPO)
    a. This is the individual who is responsible for providing data protection information and advice as well as monitoring compliance will all relevant privacy law. Within this document they will be called the **DPO**.

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
    a. Personal data must be processed in a lawful, fairly and in a transparent manner in relation to the individual.
2. Purpose limitation
    a. Personal data musty 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
    a. When collecting personal data it must be adequate, relevant and limited to what is necessary in relation to the purpose it is being collected for.
4. Accuracy
    a. We must take reasonable steps to ensure the personal data we process is as accurate up to date as possible. If personal data is incorrect or inaccurate it should be corrected, completed or erased.
5. Storage limitation
    a. Personal data should only be kept for as long as is necessary for the purpose it is being processed for.
6. Integrity and confidentiality
    a. 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 basis' for processing, each basis is equal and should be assigned on a processing by processing basis. The six lawful basis 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 parties **Legitimate Interest** where those interests are not incompatible 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 (Vision, ABC and Smart), the majority of our processing is on the basis of thesecond 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 of processing data, a Legitimate Interest Assessment will be completed and reviewed annually.

We record the lawful basis for processing alongside eachactivity in our Record of Processing Activities (RoPA) documented on spreadsheets stored in OneDrive.
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 13** 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 subjects' 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.

At Vision, ABC and Smart, each company dealing with Data Subject Requestwill follow their own process led by their Data Champions. Where individuals have questions about their process, the Data Champions should be the first point of contact.

Each team will maintain accountability for the requests they are processing by recording them in access controlled spreadsheets.

Receiving a request from an individual

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

Unlike previous laws, 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 your Data Champion immediately.

All requests received from individuals should be passed on to your Data Champion using the relevant dpo@ inbox.

Not all rights are absolute so when complex requests are received the Data Champion actioning the request should alert the DPL immediately. This should be done via email to jo.betteley@visionforeducation.co.uk.

7. Data Controller or Data Processor?

The organisation has different obligations 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 about this can be found in section 8 of this policy. Prior to the onboarding of any new third party that will process personal data, the DPL 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 the OneDrive. Access to these documents will be a 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 DPL.

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 DPL of any changes via their Data Champion.

The organisation's RoPA is stored on spreadsheets stored in OneDrive and this is maintained by the DPL and Data Champions. Each Data Champion is responsible for the upkeep and accuracy of the RoPA and will be asked to confirm they have done this on a quarterly basis.

New Vendor Onboarding Procedure

When entering into a new contract with a company where personal data is shared with the company:

1. Contract/Data Processing Agreement* should be sent to DPL to review before signing
2. DPL reviews document against contract review checklist
3. If checklist is completed satisfactorily, DPL returns contract to be signed
4. If a contract/Data Processing Agreement is not provided, DPL to contact company to ask the company:
    a. To specify the personal data which will be shared
    b. To provide a Data Sharing Agreement
5. If a Data Sharing Agreement is provided
    a. DPL to check the DSA against the contract review checklist
    b. If checklist is completed satisfactorily, DPL signs the DSA and returns contract to be signed
6. If Contract/Data Processing Agreement provided is not adequate
    a. DPL to go back to company to request inclusion of missing elements
7. If the company do not have a Data Sharing Agreement
    a. DSL to provide our standard DSA to the company
    b. Once this has been signed by the DPL and the company, DPL returns contract to be signed

* This document may be called:

- Data Processing Agreement
- Data Sharing Agreement
- Data Processing/Sharing Agreement/Terms/Annexe

9. Data Protection by design and by default

Data Protection by design and by 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 DPL and/or Data Champions 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 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 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 Champion and/or DPL should be alerted so that a DPIA can be activated.

Procedure for completing DPIA

Once it has been established that a DPIA is required, the DPL alongside the relevant Data Champion (where appropriate) will complete the DPIA template (the DPIA template on The Hub should be used). They will consult the IT Manager, 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 followed:

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
    i. 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, 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 ICO

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

The following template should be used for completing a DPIA.

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.

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 DPL.

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 DPL 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 included on outgoing references and will be shared with all future placement schools where relevant and for 3 years after they cease to work for the company.

Information regarding allegations which are found to be unsubstantiated, unfounded or malicious will not be shared.

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

13. Sending electronic marketing messages to individuals

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

We must have an individual's consent to contact them via phone, email, text or any other form of communication. 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.

Marketing templates created by the Marketing team will include the option for recipients to update their contact preferences/unsubscribe.

14. Restricted transfers of personal data outside of the EEA

A transfer of personal data to a country outside of the EEA (European Economic Area) can only take place under limited circumstances. A transfer of personal data outside of the EEA 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 EEA, the DPL should be alerted.

14. 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 Data Champion.

All personal data breaches should be reported internally only. Where necessary, the DPL will inform the ICO of the breach.

15. 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 DPL.

16. Contacting your Data Protection Team

Should you have a specific question relating to this policy please address it to the following:

Jo Betteley - DPL	jo.betteley@visionforeducation.co.uk
Vision for Education	dpo@visionforeducation.co.uk
SMART	dpo@smartteachers.co.uk
ABC	dpo@abc-teachers.co.uk